

특 2002-0025229

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
G11B 20/10

(11) 공개번호 특 2002-0025229
(43) 공개일자 2002년 04월 03일

(21) 출원번호 10-2002-7002189
(22) 출원일자 2002년 02월 20일
 번역문제출일자 2002년 02월 20일
(86) 국제출원번호 PCT/JP2001/05326 (87) 국제공개번호 WO 2001/99332
(86) 국제출원출원일자 2001년 06월 21일 (87) 국제공개일자 2001년 12월 27일
(81) 지정국
 국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아-헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀란드, 영국, 그리스, 헝가리, 이스라엘, 아이슬란드, 케냐, 키르기즈, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 라미베리아, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크메니스탄, 터키, 트리니다드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투갈, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 아랍에미리트, 안티구아바루다, 코스타리카, 도미니카연방, 알제리, 모로코, 탄자니아, 남아프리카, 벨리즈, 모잠비크, 에쿠아도르, 인도네시아, 인도, 콜롬비아, 그레나다, 감비아, 유고슬라비아, 크로아티아, 짐바브웨, 가나, 시에라리온, AP, APIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 시에라리온, 가나, 감비아, 짐바브웨, 모잠비크, 탄자니아
 EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르기즈, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크메니스탄
 EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투갈, 스웨덴, 핀란드, 사이프러스, 터키
 OA DAPI특허 : 부르키나파소, 베냉, 중앙아프리카, 콩고, 코트디부아르, 카메룬, 가봉, 기네, 말리, 모리타니, 니제르, 세네갈, 차드, 토고, 기네비소

(30) 우선권주장 JP-P-2000-00186174 2000년 06월 21일 일본 (JP)
JP-P-2000-00186175 2000년 06월 21일 일본 (JP)
(71) 출원인 소니 가부시끼 가이샤, 이데이 노부유키
일본국 도쿄도 시나가와구 기타시나가와 6초메 7반 35고
(72) 발명자 아사노, 도모유키
일본 141-0001도쿄도시나가와구기타시나가와6초메7-35소니가부시끼가이샤내 오사와, 요시토모
일본 141-0001도쿄도시나가와구기타시나가와6초메7-35소니가부시끼가이샤내 이시구로, 류지
일본 141-0001도쿄도시나가와구기타시나가와6초메7-35소니가부시끼가이샤내 미즈자와, 아즈시
일본 141-0001도쿄도시나가와구기타시나가와6초메7-35소니가부시끼가이샤내 오이시, 다테오
(74) 대리인 일본 141-0001도쿄도시나가와구기타시나가와6초메7-35소니가부시끼가이샤내 장수길, 구영창

심사청구 : 없음

(54) 정보 기록/재생 장치 및 방법

요약

본 발명은, 최신 버전의 키 경신 블록(KRB)을 선택적으로 사용하여 콘텐츠를 암호화하여 기록 매체에 저장하는 정보 기록/재생 장치 및 방법으로서, 복수의 다른 세대, 버전을 갖는 KRB를 기록 매체에 저장하는 구성을 구비한다. 이 장치 및 방법은, 최신의 KRB를 검출한 경우에는, 기록 재생 장치 내의 메모리에 저

장한다. 기록 매체에의 콘텐츠 저장 처리에 있어서는, 기록 재생 장치의 메모리 내의 KRB, 기록 매체 상의 복수의 KRB 중으로부터, 이용 가능한 최신 KRB를 검출하여, 암호 처리용 키, 예를 들면 미디어 키를 취득하여, 콘텐츠의 암호 처리를 실행한다. 따라서, 언제나 보다 새로운 버전의 KRB에 기초하는 암호화 콘텐츠를 기록 매체에 저장하는 것이 가능해진다.

도표

도면

부호어

기록 매체, 프로그램, 키 갱신 블록, 리프 키, 노드 키, 미디어 키, 디바이스 키, 버전, 콘텐츠

명세서

기술분야

본 발명은 정보 기록 장치, 정보 재생 장치, 정보 기록 방법, 정보 재생 방법, 암호 처리 키 갱신 방법, 및 정보 기록 매체와 컴퓨터 프로그램에 관한 것으로, 트리 구조의 계층적 키 배신 방식을 이용하여 마스터 키 혹은 미디어 키 등의 암호 키 갱신을 행하고, 또한, 기록 매체에 새롭게 저장되는 콘텐츠에 관하여, 보다 새로운 키를 이용한 암호화를 가능하게 한 구성에 관한 것이다.

배경기술

디지털 신호 처리 기술의 진보, 발전에 따라 최근에는, 정보를, 디지털적으로 기록하는 기록 장치나 기록 매체가 보급되어 가는 추세이다. 이러한 디지털 기록 장치 및 기록 매체에 따르면, 예를 들면, 화상이나 음성을 열화시키지 않고 기록, 재생을 반복하는 것이 가능하다. 이와 같이 디지털 데이터는 화질이나 음질을 유지한 상태 그대로 몇 번이나 복사를 반복하여 실행할 수 있기 때문에, 복사가 위법으로 행해진 기록 매체가 시장에 유통되면, 음악, 영화 등 각종 콘텐츠의 저작권자, 혹은 정당한 판매권자 등의 이익에 해를 입힐 수 있다. 최근에는, 이러한 디지털 데이터의 부정한 복사를 방지하기 위해, 디지털 기록 장치 및 기록 매체에 위법인 복사를 방지하기 위한 다양한 시스템이 도입되어 있다.

예를 들면, MD(미니 디스크: MD는 상표) 장치에서, 위법인 복사를 방지하는 방법으로서, SCMS(Serial Copy Management System)가 채용되어 있다. SCMS는 데이터 재생측에서, 오디오 데이터와 함께 SCMS 신호를 디지털 인터페이스(DIF)로부터 출력하고, 데이터 기록측에서, 재생측으로부터의 SCMS 신호에 기초하여 재생측으로부터의 오디오 데이터의 기록을 제어함으로써 위법인 복사를 방지하는 시스템이다.

구체적으로는 SCMS 신호는, 오디오 데이터가 몇 번이라도 복사가 허용되는 무제한 복사(copy free)의 데이터인지, 1번만 복사가 허용되어 있는(copy once allowed) 데이터인지, 또는 복사가 금지되어 있는(copy prohibited) 데이터인지를 나타내는 신호이다. 데이터 기록측에서, DIF로부터 오디오 데이터를 수신하면, 그 오디오 데이터와 함께 송신되는 SCMS 신호를 검출한다. 그리고, SCMS 신호가 무제한 복사(copy free)로 되어 있는 경우에는, 오디오 데이터를 SCMS 신호와 함께 미니 디스크에 기록한다. 또한, SCMS 신호가 복사를 1번만 허가(copy once allowed)로 되어 있는 경우에는, SCMS 신호를 복사 금지(copy prohibited)로 변경하여, 오디오 데이터와 함께 미니 디스크에 기록한다. 또한, SCMS 신호가 복사 금지(copy prohibited)로 되어 있는 경우에는, 오디오 데이터의 기록을 행하지 않는다. 이러한 SCMS를 사용한 제어를 행함으로써, 미니 디스크 장치에서는, SCMS에 의해 저작권을 갖는 오디오 데이터가 위법으로 복사되는 것을 방지하도록 되어 있다.

SCMS는, 상술된 바와 같이 SCMS 신호에 기초하여 재생측으로부터의 오디오 데이터의 기록을 제어하는 구성을 데이터 기록하는 기기 자체가 갖고 있는 것이 전체이기 때문에, SCMS의 제어를 실행하는 구성을 갖지 않는 미니 디스크 장치가 제조된 경우에는, 대처하는 것이 곤란해진다. 그래서, 예를 들면, DVD 플레이어에서는 콘텐츠 스크램블 시스템을 채용함으로써, 저작권을 갖는 데이터의 위법 복사를 방지하는 구성으로 되어 있다.

콘텐츠 스크램블 시스템에서는, DVD-ROM(Read Only Memory)에 비디오 데이터나 오디오 데이터 등이 암호화되어 기록되어 있으며, 그 암호화된 데이터를 복호하는 데 이용하는 키(복호 키)가, 라이선스를 받은 DVD 플레이어에게 제공된다. 라이선스는 부정 복사를 행하지 않는 등의 소정의 동작 규정에 따라도록 설계된 DVD 플레이어에 대하여 제공된다. 따라서, 라이선스를 받은 DVD 플레이어에서는, 제공된 키를 이용하여 DVD-ROM에 기록된 암호화 데이터를 복호함으로써 DVD-ROM으로부터 화상이나 음성을 재생할 수 있다.

한편, 라이선스를 받고 있지 않은 DVD 플레이어는, 암호화된 데이터를 복호하기 위한 키를 갖고 있지 않기 때문에, DVD-ROM에 기록된 암호화 데이터의 복호를 행할 수 없다. 이와 같이, 콘텐츠 스크램블 시스템 구성에서는, 라이선스 시에 요구되는 조건을 충족시키고 있지 않은 DVD 플레이어는, 디지털 데이터를 기록한 DVD-ROM의 재생을 행할 수 없게 되어, 부정 복사가 방지되도록 되어 있다.

그러나, DVD-ROM에서 채용되어 있는 콘텐츠 스크램블 시스템은, 사용자에 의한 데이터의 기밀이 불가능한 기록 매체(이하, 적절히 ROM 미디어라고 함)를 대상으로 하고 있으며, 사용자에 의한 데이터의 기밀이 가능한 기록 매체(이하, 적절히 RAM 미디어라고 함)에의 적용에 대해서는 고려되어 있지 않다.

즉, ROM 미디어에 기록된 데이터가 암호화되어 있더라도, 그 암호화된 데이터를, 그대로 전부 RAM 미디어에 복사한 경우에는, 라이선스를 받은 정당한 장치에서 재생 가능한, 소위 해적판을 작성할 수 있게 된다.

그래서, 본 출원인은, 선평출원, 특개평11-224461호 공보(특원평10-25310호)에서, 개개의 기록 매체를

식별하기 위한 정보(이하, 매체 식별 정보라 기술함)를, 다른 데이터와 함께 기록 매체에 기록하고, 정당한 라이선스를 받고 있는 장치만 기록 매체의 매체 식별 정보에 액세스가 가능해지는 구성을 제안하였다.

이 방법에서는, 기록 매체 상의 데이터는 매체 식별 정보와 라이선스를 받게 됨으로써 얻어지는 비밀 키(마스터 키)에 의해 암호화되고, 라이선스를 받고 있지 않은 장치가, 이 암호화된 데이터를 판독하였다고 해도, 의미가 있는 데이터를 얻는 것이 불가능하게 되어 있다. 또, 장치는 라이선스를 받을 때, 부정행위(위법 복사)를 할 수 없도록 그 동작이 규정된다.

라이선스를 받고 있지 않은 장치는, 매체 식별 정보에 액세스할 수 없으며, 또한, 매체 식별 정보는 개개의 매체마다 개별적인 값으로 되어 있기 때문에, 라이선스를 받고 있지 않은 장치가 기록 매체에 기록되어 있는, 암호화된 데이터의 전부를 새로운 기록 매체에 복제하였다고 해도, 그러한 방법으로 작성된 기록 매체에 기록된 데이터는, 라이선스를 받고 있지 않은 장치는 물론, 라이선스를 받은 장치에서도 정확하게 복호할 수 없기 때문에, 실질적으로 위법 복사가 방지되게 된다.

그런데, 상기한 구성에서는, 라이선스를 받은 장치에서 저장되는 마스터 키는 전체 기기에서 공통적인 것이 일반적이다. 이와 같이 복수의 기기에 대하여 공통의 마스터 키를 저장하는 것은, 하나의 기기로 기록된 매체를 다른 기기로 재생가능하게 하기(상호 운용성을 확보하기) 위해 필요한 조건이기 때문이다.

이러한 방식에서는, 공격자가 하나의 기기의 공격에 성공하고, 마스터 키를 추출한 경우, 전체 시스템에서 암호화되어 기록되어 있는 데이터를 복호할 수 있게 되어, 시스템 전체가 붕괴된다. 이것을 방지하기 위해서는, 어떠한 기기가 공격되어 마스터 키가 노출한 것이 발각된 경우, 마스터 키를 새로운 것으로 갱신하고, 공격에 굴복한 기기 이외의 전체 기기에 새롭게 갱신된 마스터 키를 제공하는 것이 필요하게 된다. 이 구성을 실현하는 가장 단순한 방식으로는, 개개의 기기에 고유의 키(디바이스 키)를 제공해 놓고, 새로운 마스터 키를 개개의 디바이스 키로 암호화한 값을 준비하고, 기록 매체를 통해 기기 간 전송하는 방식이 고려되지만, 기기의 대수에 비례하여 전송하여야 할 전체 메시징량이 증가한다고 하는 문제가 있다.

상기 문제를 해결하는 구성으로서, 본 출원인은 각 정보 기록 재생 장치를 n개의 트리의 각 리프(leaf)에 배치한 구성의 키 배신 방법을 이용하며, 기록 매체 혹은 통신 회선을 통해 콘텐츠 데이터의 기록 매체로의 기록 혹은 기록 매체로부터의 재생에 필요한 키(마스터 키 혹은 미디어 키)를 배신하고, 이것을 이용하여 각 장치가 콘텐츠 데이터의 기록, 재생을 행하도록 함으로써, 정당한(비밀이 노출되지 않은) 장치에 대하여 적은 메시징량으로 마스터 키 혹은 미디어 키를 전송할 수 있는 구성을 먼저 제안하여, 이미 특허 출원(특원평2000-105328)하고 있다. 구체적으로는, 기록 매체에서의 기록 혹은 기록 매체로부터의 재생에 필요한 키를 생성하기 위해 필요한 키, 예를 들면 n개의 트리의 각 리프를 구성하는 노드에 할당된 노드 키를 갱신 노드 키로서 설정하고, 갱신 노드 키를 정당한 기기만이 갖는 리프 키, 노드 키로 복호 가능한 상태로 암호화 처리한 정보를 포함하는 키 갱신 블록(KRB: Key Renewal Block)을 각 정보 기록 재생 장치에 배신(配信)하고, 키 갱신 블록(KRB)을 수신한 각 정보 기록 재생 장치의 KRB 복호 처리에 의해, 각 장치가 기록 혹은 기록 매체로부터의 재생에 필요한 키를 취득 가능하게 한 구성이다.

상기 구성은, 특정한 시스템(기록 재생 장치 그룹) 중 임의의 장치가 공격자의 공격을 받아, 그 비밀인 디바이스 키가 노출된 것이 발각된 경우, 그 이후에 제조하는 기록 매체에서는, 비밀이 노출된 기록 재생 장치를 시스템으로부터 배제하는, 즉, 배제되어 있지 않은 장치와의 기록 재생의 호환성을 얻을 수 없다고 하는 특징을 갖는다.

이 구성에서는, 비밀이 노출된 기기를 시스템으로부터 배제할 수 있는 것은, 그것이 발각한 이후에 제조되는 기록 매체에서만으로, 그 이전에 제조된 기록 매체에서는, 실제로 데이터를 기록하는 것이, 상기한 발각 시점 이후라고 해도, 기록된 데이터를, 노출된 키로 복호할 수 있게 되는, 즉, 배제하여야 할 장치를 실제로 배제할 수 있는 경우가 적다고 하는 과제가 있다.

〈발명의 개시〉

본 발명은 상술의 문제를 해결하는 것으로, 비밀이 노출된 것이 발각된 이후, 그 이전에 제조된 기록 매체에서도 기록된 데이터를 노출된 키로 복호할 수 없도록 하는 것을 가능하게 하며, 보다 유효한 콘텐츠 암호화를 가능하게 한 정보 기록 장치, 정보 재생 장치, 정보 기록 방법, 정보 재생 방법, 암호 처리 키 갱신 방법, 및 정보 기록 매체와 컴퓨터 프로그램을 제공하는 것이다.

상술한 바와 같은 목적을 달성하기 위해 제안되는 본 발명은, 기록 매체에 정보를 기록하는 정보 기록 장치로서, 이 장치는, 복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과, 정보 기록 장치에 내장한 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하며, 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하고, 이 산출된 암호 처리용 키를 사용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 암호 처리 수단을 포함한다. 이 장치의 암호 처리 수단은, 기록 매체에 대한 콘텐츠의 암호화 및 저장 처리에서, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신의 키 갱신 블록을 검출하여, 검출된 이용 가능한 최신의 키 갱신 블록의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행한다.

또한, 본 발명은 기록 매체로부터 정보를 재생하는 정보 재생 장치로서, 이 장치는 복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과, 이 정보 재생 장치에 내장한 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하며, 기록 매체에 저장된 암호 데이터의 복호 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하고, 이 산출된

암호 처리용 키를 사용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 암호 처리 수단을 포함한다. 이 장치에서, 암호 처리 수단은 기록 매체에 저장된 암호 데이터의 복호 처리에서, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하여, 검출된 키 갱신 블록의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행한다.

본 발명은, 복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하고, 기록 매체에 대한 정보 기록을 행하는 정보 기록 장치에서의 정보 기록 방법으로서, 이러한 방법은, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신의 키 갱신 블록을 검출하는 검출 단계와, 검출 단계에서 검출된 이용 가능한 최신의 키 갱신 블록에 대하여 정보 기록 장치에 내장한 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 키 갱신 블록의 복호 처리를 실행하여, 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하는 복호 처리 단계와, 복호 처리 단계에서, 산출된 암호 처리용 키를 이용하여 기록 매체에 대한 기록 데이터의 암호화를 행하여 기록 매체에 저장하는 단계를 포함한다.

또한, 본 발명은, 복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 보유하고, 기록 매체에 저장된 암호 데이터의 복호 처리를 행하는 정보 재생 장치에서의 정보 재생 방법으로서, 기록 매체에 저장되며, 재생 대상이 되는 콘텐츠의 암호 처리용 키의 버전 정보를 취득하는 단계와, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중에서 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하는 검출 단계와, 검출 단계에서 검출된 키 갱신 블록의 복호 처리에 의해 암호 처리용 키를 생성하는 단계와, 생성된 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 단계를 포함한다.

또한, 본 발명은 정보를 기록 가능한 정보 기록 매체로서, 복수의 다른 정보 기록 장치 또는 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 또는 재생 장치 고유의 리프 키에 포함되는 갱신 노드 키를 하위 계층의 노드 키 또는 리프 키 중 적어도 어느 하나를 포함하는 키에 의해 암호화한 키 갱신 블록을, 다른 구성을 갖는 복수의 키 갱신 블록으로서 저장하고 있다.

또한, 본 발명은 복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하고, 기록 매체에 대한 정보 기록을 행하는 정보 기록 장치에서의 정보 기록 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램으로서, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신의 키 갱신 블록을 검출하는 검출 단계와, 검출 단계에서 검출된 이용 가능한 최신의 키 갱신 블록에 대하여, 정보 기록 장치에 내장한 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 키 갱신 블록의 복호 처리를 실행하여, 상기 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하는 복호 처리 단계와, 복호 처리 단계에서, 산출된 암호 처리용 키를 이용하여 상기 기록 매체에 대한 기록 데이터의 암호화를 행하여 기록 매체에 저장하는 단계를 포함한다.

또한, 본 발명은 복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 보유하고, 기록 매체에 저장된 암호 데이터의 복호 처리를 행하는 정보 재생 장치에서의 정보 재생 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램으로서, 기록 매체에 저장되고, 재생 대상이 되는 콘텐츠의 암호 처리용 키의 버전 정보를 취득하는 단계와, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하는 검출 단계와, 검출 단계에서 검출된 키 갱신 블록의 복호 처리에 의해 암호 처리용 키를 생성하는 단계와, 생성된 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 단계를 포함한다.

또한, 본 발명은 기록 매체에 정보를 기록하는 정보 기록 장치로서, 복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과, 정보 기록 장치에 내장한 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하여, 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하고, 이 산출된 암호 처리용 키를 사용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 암호 처리 수단과, 기록 매체에 대한 액세스 시에 기록 매체에 저장된 키 갱신 블록과, 정보 기록 장치 자신이 갖는 키 갱신 블록과의 버전 비교를 실행하고, 신 버전의 키 갱신 블록이 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록으로서, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에서, 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 수단을 포함한다.

또한, 본 발명은 기록 매체로부터 정보를 재생하는 정보 재생 장치에서, 복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과, 정보 재생 장치에 내장한 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하여, 상기 기록 매체에 저장된 암호 데이터의 복호 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하고, 이 산출된 암호 처리용 키를 사용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 암호 처리 수단과, 기록 매체에 대한 액세스 시에 기록 매체에 저장된 키 갱신 블록과 정보 재생 장치 자신이 갖는 키 갱신 블록과의 버전 비교를 실행하고, 신 버전의 키 갱신 블록이 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록으로서, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에서 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 수단을 포함한다.

또한, 본 발명은 복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의

노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하고, 기록 매체에 대한 정보 기록을 행하는 정보 기록 또는 재생 장치에서의 암호 처리 키 갱신 방법으로서, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신 버전의 키 갱신 블록을 검출하는 검출 단계와, 최신 버전의 키 갱신 블록이 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록으로서, 이 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에서 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 단계를 포함한다.

그리고, 본 발명은 복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하고, 기록 매체에 대한 정보 기록, 재생을 행하는 정보 기록 또는 재생 장치에서의 암호 처리 키 갱신 블록을 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램으로서, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신 버전의 키 갱신 블록을 검출하는 검출 단계와, 최신 버전의 키 갱신 블록이 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록으로서, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에서 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 단계를 포함한다.

본 발명의 구성에서는, 트리(나무) 구조의 계층적 키 배신 방식을 이용함으로써, 키 갱신에 필요한 배신 메시징량을 크게 억제하고 있다. 즉, 각 기기를 n개의 트리의 각 리프에 배치한 구성의 키 배신 방식을 이용하여, 기록 매체 혹은 통신 회선을 통해 콘텐츠 데이터의 기록 매체로의 기록 혹은 기록 매체로부터의 재생에 필요한 키(마스터 키 혹은 미디어 키)를 배신하고, 이것을 이용하여 각 장치가 콘텐츠 데이터의 기록, 재생을 행한다.

또한, 본 발명에서는, 전송한 과제를 해결하기 위해 기록 매체마다 단 하나의 미디어 키를 설정하는 것이 아니라, 복수의 미디어 키를 설정할 수 있도록 한다. 즉, 기록 매체가 제조되어 시장에 나온 후에도, 보다 새로운 미디어 키를 산출하기 위한 키 갱신 블록(KRB)을 기록 재생 장치가 기록 매체에 기입할 수 있도록 한다. 데이터를 기록 매체에 기록할 때에는, 기록 재생 장치는 기록 매체 상의 키 갱신 블록(KRB)과, 자신이 저장하는 KRB 중 최신의 것을 이용하여 미디어 키를 산출하여 데이터의 암호화에 사용하고, 또한 그 최신의 KRB가 기록 매체 상에는 없이 자신이 저장하고 있는 것이면, 그것을 기록 매체에 저장하도록 한다.

또한, 본 발명의 기록 재생 장치는 기록 매체에 액세스할 때 기록 매체 상의 모든 KRB의 버전을 조사하여, 그 중 최신의 것이 자신이 저장하는 것보다 새로운 것이면, 이를 이용하여 자신이 저장하는 KRB를 최신의 것으로 갱신한다. 이를 처리에 의해 기록 재생 장치에는 점점 새로운 KRB가 저장되고, 또한 데이터가 기록될 때에는 그 시점에서 기록 재생 장치와 기록 매체에 저장하는 최신의 KRB에 의해 산출되는 미디어 키를 이용하여 데이터가 암호화되어 기록되기 때문에, 예를 들면 기록 매체가 제조된 것이 매우 오래되고, 사전에 기록 매체에 저장되어 있는 KRB가 오래된 것이었다고 해도, 데이터가 기록되는 때는 새로운 KRB가 사용될 가능성이 높기 때문에, 그 데이터의 안전성을 보다 높게 지키는 것이 가능해진다.

또한, 본 발명에서는, 전송한 과제를 해결하기 위해 복수의 세대(世代), 버전이 다른 키를 기록 매체에 저장 가능하게 하고, 기록 재생 장치가 기록 매체에 액세스했을 때, 보다 새로운 키를 기록 매체에 저장하여, 불필요 키를 삭제하는 구성으로 하고 있다. 기록 매체가 제조되어 시장에 나온 후에도, 보다 새로운 미디어 키를 산출하기 위한 키 갱신 블록(KRB)을 기록 재생 장치가 기록 매체에 기입할 수 있도록 한다. 데이터를 기록 매체에 기록할 때에는 기록 재생 장치는 기록 매체 상의 키 갱신 블록(KRB)과, 자신이 저장하는 KRB 중 최신의 것을 이용하여 미디어 키를 산출하여 데이터의 암호화에 사용하고, 또한 그 최신의 KRB가 기록 매체 상에는 없이 자신이 저장하고 있는 것이면, 그것을 기록 매체에 저장하도록 한다.

또한, 본 발명의 기록 재생 장치는, 새로운 KRB의 기록 매체로의 기록을, 콘텐츠 데이터를 기록할 때뿐만 아니라, 기록 매체가 기록 재생 장치에 장착되고, 기록 재생 장치가 기록 매체에 액세스할 때 행하도록 한다. 이와 같이 함으로써, 기록 매체에 저장되어 있는 모든 KRB보다도 새로운 KRB를 갖는 기록 재생 장치는 콘텐츠 데이터를 기록하지 않은 경우에도, 새로운 KRB를 기록 매체에 기록할 수 있게 되어, 이 때문에, 새로운 KRB의 마이그레이션 속도가 빠르게 된다. 또한, 기록 매체 상의 콘텐츠 데이터의 암호화에는 사용되어 있지 않고, 또한, 그 기록 매체 상의 KRB 중 최신이 아닌 KRB가, 하나 또는 복수, 기록 매체 상에 남는 것이 고려되지만, 이들 KRB를 기록 재생 장치가 소거함으로써, 기록 매체의 기록 용량을 절약하는 것이 가능해진다.

또, 본 발명의 프로그램 제공 매체는, 예를 들면, 다양한 프로그램 코드를 실행 가능한 범용 컴퓨터 시스템에 대하여, 컴퓨터 프로그램을 컴퓨터로 판독 가능한 형식으로 제공하는 매체이다. 매체는 CD나 FD, MO 등의 기록 매체, 혹은, 네트워크 등의 전송 매체 등으로 그 형태는 특별히 한정되지 않는다.

이와 같은 프로그램 제공 매체는, 컴퓨터 시스템 상에서 소정의 컴퓨터 프로그램의 기능을 실현하기 위한, 컴퓨터 프로그램과 제공 매체와의 구조 상 또는 기능 상의 협동적 관계를 정의한 것이다. 다시 말하면, 그 제공 매체를 통해 컴퓨터 프로그램을 컴퓨터 시스템에 인스톨함으로써, 컴퓨터 시스템 상에서는 협동적 작용이 발휘되고, 본 발명의 다른 측면과 마찬가지로의 작용 효과를 얻는 것이 가능한 것이다.

본 발명의 또 다른 목적, 특징이나 이점은 후술하는 본 발명의 실시예나 첨부하는 도면에 기초한, 보다 상세한 설명에 의해 명백하게 될 것이다.

도면의 간단한 설명

도 1은 본 발명의 정보 기록 재생 장치의 구성예를 나타내는 블록도.

도 2A 및 도 2B는 본 발명의 정보 기록 재생 장치의 데이터 기록 처리 흐름을 나타내는 도면.

도 3A 및 도 3B는 본 발명의 정보 기록 재생 장치의 데이터 재생 처리 흐름을 나타내는 도면.

도 4는 본 발명의 정보 기록 재생 장치에 대한 미디어 키 등의 키의 암호화 처리에 대하여 설명하는 트리 구성도.

도 5A 및 도 5B는 본 발명의 정보 기록 재생 장치에 대한 미디어 키 등의 키의 배포에 사용되는 키 갱신 블록(KRB)의 예를 나타내는 도면.

도 6은 정보 기록 재생 장치에서의 미디어 키의 키 갱신 블록(KRB)을 사용한 배포예와 복호 처리예를 나타내는 도면.

도 7은 본 발명의 정보 기록 재생 장치에서의 미디어 키를 사용한 데이터 기록 처리 시의 암호화 처리를 설명하는 블록도.

도 8은 본 발명의 정보 기록 재생 장치에서 적용 가능한 디스크 고유 키의 생성예를 설명하는 도면.

도 9는 본 발명의 정보 기록 재생 장치에서 적용 가능한 타이틀 고유 키의 생성 처리예를 나타내는 도면.

도 10은 본 발명의 정보 기록 재생 장치에서 적용 가능한 블록 키의 생성 방법을 설명하는 도면.

도 11은 본 발명의 정보 기록 재생 장치에서의 미디어 키를 사용한 데이터 재생 처리 시의 복호 처리를 설명하는 블록도.

도 12는 본 발명의 정보 기록 재생 장치에서 사용되는 키 갱신 블록(KRB)의 포맷예를 나타내는 도면.

도 13은 본 발명의 정보 기록 재생 장치에서 사용되는 키 갱신 블록(KRB)의 태그의 구성을 설명하는 도면.

도 14의 (A) 및 (B)는 본 발명의 정보 기록 재생 장치에서 키 갱신 블록(KRB)을 복수 저장한 기록 매체, 및 기록 재생 장치에서의 키 갱신 블록(KRB)의 갱신 처리를 설명하는 도면.

도 15는 본 발명의 정보 기록 재생 장치에서의 키 갱신 블록(KRB)의 갱신 처리를 설명하는 흐름도.

도 16A 및 도 16B는 본 발명의 정보 기록 재생 장치에서 키 갱신 블록(KRB)을 복수 저장한 기록 매체, 및 최신의 키 갱신 블록(KRB)을 이용하여 취득되는 키에 의한 암호화를 행한 콘텐츠의 저장 처리를 설명하는 도면.

도 17은 본 발명의 정보 기록 재생 장치에서의 키 갱신 블록(KRB)을 이용하여 취득되는 키에 의한 암호화, 콘텐츠의 저장 처리를 설명하는 흐름도.

도 18은 본 발명의 정보 기록 재생 장치에서의 키 갱신 블록(KRB)을 이용하여 취득되는 키에 의한 복호, 및 콘텐츠의 재생 처리 수순을 설명하는 흐름도.

도 19A 및 도 19B는 본 발명의 정보 기록 재생 장치에서 기록 재생 장치에 저장한 키 갱신 블록(KRB)의 갱신 처리를 설명하는 도면.

도 20A 및 도 20B는 본 발명의 정보 기록 재생 장치에서 기록 매체에 저장한 키 갱신 블록(KRB)의 갱신 처리를 설명하는 도면.

도 21A 및 도 21B는 본 발명의 정보 기록 재생 장치에서 기록 매체에 저장한 키 갱신 블록(KRB)의 삭제 처리를 설명하는 도면.

도 22는 본 발명의 정보 기록 재생 장치에서의 키 갱신 블록(KRB)의 갱신, 삭제 처리를 설명하는 흐름도.

도 23은 본 발명의 정보 기록 재생 장치에서의 키 갱신 블록(KRB)을 이용하여 취득되는 키에 의한 암호화, 및 콘텐츠의 저장 처리 수순을 설명하는 흐름도.

도 24는 본 발명의 정보 기록 재생 장치에서의 키 갱신 블록(KRB)을 이용하여 취득되는 키에 의한 복호, 및 콘텐츠의 재생 처리 수순을 설명하는 흐름도.

도 25A 및 도 25B는 본 발명의 정보 기록 재생 장치에서의 데이터 기록 처리 시의 복사 제어 처리를 설명하는 흐름도.

도 26A 및 도 26B는 본 발명의 정보 기록 재생 장치에서의 데이터 재생 처리 시의 복사 제어 처리를 설명하는 흐름도.

도 27은 본 발명의 정보 기록 재생 장치에서, 데이터 처리를 소프트웨어에 의해 실행하는 경우의 처리 수단의 구성을 나타낸 블록도.

〈발명을 실시하기 위한 최량의 형태〉

이하, 본 발명의 구체적인 구성을 도면을 참조하여 설명한다.

도 1은 본 발명을 적용한 기록 재생 장치(100)의 일 실시예 구성을 나타내는 블록도이다. 기록 재생 장치(100)는 입출력 I/F(Interface: 120), MPEG(Moving Picture Experts Group)코덱(130), A/D, D/A 컨버터(141)를 구비한 입출력 I/F(Interface: 140), 암호 처리 수단(150), ROM(Read Only Memory: 160), CPU(Central Processing Unit: 170), 메모리(180), 기록 매체(195)의 기록 매체 인터페이스(I/F: 190)를 구비하고, 이들은 버스(110)에 의해 상호 접속되어 있다.

입출력 I/F(120)는 외부로부터 공급되는 화상, 음성, 프로그램 등의 각종 콘텐츠를 구성하는 디지털 신호를 수신하여 버스(110) 상에 출력함과 함께, 버스(110) 상의 디지털 신호를 수신하여 외부로 출력한다. MPEG 코덱(130)은 버스(110)를 통해 공급되는 MPEG 부호화된 데이터를 MPEG 디코드하고, 입출력 I/F(140)로 출력함과 함께 입출력 I/F(140)로부터 공급되는 디지털 신호를 MPEG 인코드하여 패스(110) 상으로 출력한다. 입출력 I/F(140)는 A/D, D/A 컨버터(141)를 내장하고 있다. 입출력 I/F(140)는 외부로부터

공급되는 콘텐츠로서의 아날로그 신호를 수신하고, A/D, D/A 컨버터(141)로 A/D(Analogue Digital) 변환함으로써 디지털 신호로서 MPEG 코덱(130)으로 출력함과 함께, MPEG 코덱(130)으로부터의 디지털 신호를 A/D, D/A 컨버터(141)로 D/A(Digital Analogue) 변환함으로써 아날로그 신호로서 외부로 출력한다.

암호 처리 수단(150)은, 예를 들면, 1칩의 LSI(Large Scale Integrated Circuit)로 구성되며, 버스(110)를 통해 공급되는 콘텐츠로서의 디지털 신호를 암호화하거나, 또는 복호하며, 버스(110) 상으로 출력하는 구성을 갖는다. 또, 암호 처리 수단(150)은 1칩 LSI에 한하지 않고, 각종 소프트웨어 또는 하드웨어를 조합한 구성에 의해 실현하는 것도 가능하다. 소프트웨어 구성에 의한 처리 수단으로서의 구성에 대해서는 후단에서 설명한다.

ROM(160)은, 예를 들면, 기록 재생 장치마다 고유인, 혹은 복수의 기록 재생 장치의 그룹마다 고유인 디바이스 키인 리프 키와, 복수의 기록 재생 장치, 혹은 복수의 그룹에 공유의 디바이스 키인 노드 키를 기억하고 있다. CPU(170)는 메모리(180)에 기억된 프로그램을 실행함으로써, MPEG 코덱(130)이나 암호 처리 수단(150) 등을 제어한다. 메모리(180)는 예를 들면, 불휘발성 메모리로서, CPU(170)가 실행하는 프로그램이나, CPU(170)의 동작 상 필요한 데이터를 기억한다. 기록 매체 인터페이스(190)는 디지털 데이터를 기록 매체 재생 가능한 기록 매체(195)를 구동함으로써, 기록 매체(195)로부터 디지털 데이터를 판독하여(재생하여) 버스(110) 상으로 출력함과 함께, 버스(110)를 통해 공급되는 디지털 데이터를 기록 매체(195)에 공급하여 기록시킨다. 또, 프로그램을 ROM(160)에, 디바이스 키를 메모리(180)에 기억하는 구성으로 하여도 된다.

기록 매체(195)는, 예를 들면, DVD, CD 등의 광 디스크, 광 자기 디스크, 자기 디스크, 자기 테이프, 혹은 RAM 등의 반도체 메모리 등, 디지털 데이터가 기억 가능한 매체로서, 본 실시 형태에서는 기록 매체 인터페이스(190)에 대하여 착탈 가능한 구성으로 한다. 단, 기록 매체(195)는 기록 재생 장치(100)에 내장하는 구성으로 하여도 된다.

다음에, 도 1의 기록 재생 장치에서의 기록 매체에 대한 데이터 기록 처리 및 기록 매체로부터의 데이터 재생 처리에 대하여, 도 2A, 도 2B 및 도 3A, 도 3B의 흐름도를 참조하여 설명한다. 외부로부터의 디지털 신호의 콘텐츠를 기록 매체(195)에 기록하는 경우에는, 도 2A의 흐름도에 따라 기록 처리가 행해진다. 즉, 디지털 신호의 콘텐츠(디지털 콘텐츠)가, 예를 들면, IEEE(Institute of Electrical and Electronics Engineers) 1394 직렬 버스 등을 통해 입출력 I/F(120)에 공급되면, 단계 S201에서 입출력 I/F(120)는 공급되는 디지털 콘텐츠를 수신하고, 패스(110)를 통해 암호 처리 수단(150)으로 출력한다.

암호 처리 수단(150)은, 단계 S202에서 수신한 디지털 콘텐츠에 대한 암호화 처리를 실행하고, 그 결과 얻어지는 암호화 콘텐츠를 버스(110)를 통해 기록 매체 I/F(190)로 출력한다. 암호화 콘텐츠는 기록 매체 I/F(190)를 통해 기록 매체(195)에 기록(단계 S203)되고, 기록 처리를 종료한다.

또, IEEE 1394 직렬 버스를 통해 접속한 장치 상호간에서, 디지털 콘텐츠를 전송할 때의, 디지털 콘텐츠를 보호하기 위한 규격으로서, 본 특허 출원인인 소니 주식회사를 포함한 5사에 의해, 5CDTCP(Five Company Digital Transmission Content Protection)(이하, 적절하게, DTCP라고 함)가 정해져 있지만, 이 DTCP에서는, 무제한 복사가 아닌 디지털 콘텐츠를 장치 상호간에서 전송하는 경우, 데이터 전송에 앞서서, 송신측과 수신측이 복사를 제어하기 위한 복사 제어 정보를 정확하게 취급할 수 있는 지에 대한 여부의 인증을 서로 행하고, 그 후, 송신측에서 디지털 콘텐츠를 암호화하여 전송하고, 수신측에서 그 암호화된 디지털 콘텐츠(암호화 콘텐츠)를 복호하도록 되어 있다.

이 DTCP에 규격에 기초한 데이터 송수신에서는, 데이터 수신측의 입출력 I/F(120)는 단계 S201에서, IEEE 1394 직렬 버스를 통해 암호화 콘텐츠를 수신하고, 그 암호화 콘텐츠를, DTCP에 규격에 준거하여 복호하고, 평문(平文)의 콘텐츠로서, 그 후 암호 처리 수단(150)으로 출력한다.

DTCP에 의한 디지털 콘텐츠의 암호화는 시간 변화하는 키를 생성하고, 그 키를 이용하여 행해진다. 암호화된 디지털 콘텐츠는 그 암호화에 이용한 키를 포함해서, IEEE 1394 직렬 버스 상으로 전송되고, 수신측에서는, 암호화된 디지털 콘텐츠를 거기에 포함되는 키를 이용하여 복호한다.

또, DTCP에 의하면, 정확하게는 키의 초기값과, 디지털 콘텐츠의 암호화에 이용하는 키의 변경 타이밍을 나타내는 플래그가, 암호화 콘텐츠에 포함된다. 그리고, 수신측에서는 그 암호화 콘텐츠에 포함되는 키의 초기값을, 또한, 그 암호화 콘텐츠에 포함되는 플래그의 타이밍으로 변경함으로써, 암호화에 이용된 키가 생성되고, 암호화 콘텐츠가 복호된다. 단, 여기서는, 암호화 콘텐츠에 그 복호를 행하기 위한 키가 포함되어 있다고 생각하여도 지장이 없기 때문에, 이하에서는, 그와 같이 생각하도록 한다. 또, DTCP의 규격서는 DTLA(Digital Transmission Licensing Administrator)로부터 인포메이션 버전(Informational Version)을 누구라도 취득할 수 있다.

다음에, 외부로부터의 아날로그 신호의 콘텐츠를, 기록 매체(195)에 기록하는 경우의 처리에 대하여, 도 2B의 흐름도에 따라 설명한다. 아날로그 신호의 콘텐츠(아날로그 콘텐츠)가 입출력 I/F(140)에 공급되면, 입출력 I/F(140)는 단계 S221에서, 그 아날로그 콘텐츠를 수신하고, 단계 S222로 진행하며, 내장하는 A/D, D/A 컨버터(141)로 A/D 변환하여, 디지털 신호의 콘텐츠(디지털 콘텐츠)로 한다.

이 디지털 콘텐츠는 MPEG 코덱(130)에 공급되고, 단계 S223에서 MPEG 인코드, 즉 MPEG 압축에 의한 부호화 처리가 실행되고, 버스(110)를 통해 암호 처리 수단(150)에 공급된다.

이하, 단계 S224, S225에서, 도 2A의 단계 S202, S203에서의 처리와 마찬가지로의 처리가 행해진다. 즉, 암호 처리 수단(150)에서의 암호화 처리가 실행되고, 그 결과 얻어지는 암호화 콘텐츠를, 기록 매체(195)에 기록하여 기록 처리를 종료한다.

다음에, 기록 매체(195)에 기록된 콘텐츠를 재생하여, 디지털 콘텐츠, 혹은 아날로그 콘텐츠로서 출력하는 처리에 대하여 도 3A 및 도 3B의 흐름도에 따라 설명한다. 디지털 콘텐츠로서 외부로 출력하는 처리는 도 3A의 흐름도에 따라 재생 처리로서 실행된다. 즉, 우선 처음에 단계 S301에서, 기록 매체 I/F(190)에 의해 기록 매체(195)에 기록된 암호화 콘텐츠가 판독되고, 버스(110)를 통해 암호 처리 수단(150)으로 출

력된다.

암호 처리 수단(150)에서는, 단계 S302에서, 기록 매체 1/F(190)로부터 공급되는 암호화 콘텐츠가 복호 처리되고, 복호 데이터가 버스(110)를 통해, 입출력 1/F(120)에 공급된다. 단계 S303에서, 입출력 1/F(120)는 디지털 콘텐츠를 외부로 출력하고, 재생 처리를 종료한다.

또, 입출력 1/F(120)는 단계 S303에서, IEEE 1394 직렬 버스를 통해, 디지털 콘텐츠를 출력하는 경우에는, DTCP의 규격에 준거하여, 상술한 바와 같이, 상대 장치 사이에서 인증을 서로 행하고, 그 후, 디지털 콘텐츠를 암호화하여 전송한다.

기록 매체(195)에 기록된 콘텐츠를 재생하여, 아날로그 콘텐츠로서 외부로 출력하는 경우에는, 도 3B의 흐름도에 따른 재생 처리가 행해진다.

즉, 단계 S321, S322에서, 도 3A의 단계 S301, S302에서의 경우와 각각 마찬가지로 처리가 행해지고, 이에 따라, 암호 처리 수단(150)에서 얻어진 복호된 디지털 콘텐츠는 버스(110)를 통해 MPEG 코덱(130)에 공급된다.

MPEG 코덱(130)에서는, 단계 S323에서, 디지털 콘텐츠가 MPEG 디코드, 즉 신장(伸長) 처리가 실행되어, 입출력 1/F(140)에 공급된다. 입출력 1/F(140)는, 단계 S324에서, MPEG 코덱(130)으로 MPEG 디코드된 디지털 콘텐츠를, 내장하는 A/D, D/A 컨버터(141)로 D/A 변환하여, 아날로그 콘텐츠로 한다. 그리고, 단계 S325로 진행하여, 입출력 1/F(140)는 그 아날로그 콘텐츠를 외부로 출력하고, 재생 처리를 종료한다.

다음에, 도 1에 도시한 기록 재생 장치, 데이터를 기록 매체에 기록, 혹은 기록 매체로부터 재생할 때에 필요한 키, 예를 들면 마스터 키 혹은 미디어 키를, 각 기기에 배포하는 구성에 대하여 설명한다. 여기서, 마스터 키는 이 시스템에서 공통으로, 복수의 디바이스에서 공통으로 유지되는 키이며, 디바이스의 제조 시에 디바이스 내에 기록된다. 이 키 배산 시스템을 이용하는 디바이스 전부에서 공통적인 것이 바람직하다. 또한, 키인 미디어 키는, 각 기록 매체에 고유한 키이며, 기록 매체의 제조 시에 기록 매체에 기록된다. 이상적으로는 모든 기록 매체마다 다른 것이 바람직하지만, 기록 매체의 제조 공정의 제약상, 복수의 기록 매체를 그룹으로서, 그룹별로 바꾸는 것이 현실적이다. 예를 들면, 기록 매체의 제조 로트를 그룹으로서, 로트마다 미디어 키를 바꾸도록 구성하여도 된다. 이하에서는, 이들 키를 갱신하는 예를 중심으로 기술하지만, 마스터 키가 기록되어 있지 않는 디바이스 혹은 미디어 키가 기록되어 있지 않은 기록 매체에, 각각의 키를 배포 및 기록하기 위해 본 발명을 이용하는 것도 가능하다.

도 4는, 본 방식을 이용한 기록 시스템에서의 기록 재생 장치의 키 배포 구성을 나타낸 도면이다. 도 4의 최하단에 나타내는 번호 0~15가 개개의 기록 재생 장치이다. 즉, 도 4에 도시한 트리 구조의 각 리프가 각각의 기록 재생 장치에 상당한다.

각 디바이스 0~15는, 제조 시(출하 시)에, 사전에 정해져 있는 초기 트리에서의, 자신의 리프로부터 루트에 이르기까지의 노드에 할당된 키(노드 키) 및 각 리프의 리프 키를 자신에게 저장한다. 도 4의 최하단에 나타내는 K0000~K1111이 각 디바이스 0~15로 각각 할당된 리프 키이며, 최상단의 KR로부터, 최하단으로부터 2번째의 절(노드)에 기재된 키: KR~K111를 노드 키로 한다.

도 4에 도시한 트리 구성에서, 예를 들면 디바이스 0은 리프 키 K0000과, 노드 키: K000, K00, K0, KR를 소유한다. 디바이스 5는 K0101, K010, K01, K0, KR를 소유한다. 디바이스 15는 K1111, K111, K11, K1, KR를 소유한다. 또, 도 4의 트리에는 디바이스가 0~15의 16개만 기재되며, 트리 구조도 4단 구성의 균형이 잡힌 좌우 대칭 구성으로서 나타내고 있지만, 더욱 많은 디바이스가 트리 중에 구성되며, 또한, 트리의 각부에서 다른 단수 구성을 갖는 것이 가능하다.

또한, 도 4의 트리 구조에 포함되는 각 기록 재생기에는, 다양한 기록 매체, 예를 들면 DVD, CD, MO, 메모리 스틱(상표) 등을 사용하는 다양한 타입의 기록 재생기가 포함되어 있다. 또한, 다양한 어플리케이션 서비스 공존하는 것이 상정된다. 이러한 다른 디바이스, 다른 어플리케이션의 공존 구성 상에 도 4에 도시한 키 배포 구성이 적용되어 있다.

이들 다양한 디바이스, 어플리케이션이 공존하는 시스템에서, 예를 들면 도 4의 점선으로 둘러싼 부분, 즉 디바이스 0, 1, 2, 3를 동일한 포맷의 기록 매체를 이용하는 하나의 그룹으로서 설정한다. 예를 들면, 이 점선으로 둘러싼 그룹 내에 포함되는 디바이스에 대해서는, 통합하여, 공통의 콘텐츠를 암호화하여 프로바이더로부터 송부하거나, 공통으로 사용하는 마스터 키를 송부하거나, 혹은 각 디바이스로부터 프로바이더 혹은 결제 기관 등에 콘텐츠 요금의 지불 데이터를 역시 암호화하여 출력한다고 하는 처리가 실행된다. 콘텐츠 프로바이더, 혹은 결제 처리 기관 등, 각 디바이스와의 데이터 송수신을 행하는 기관은, 도 4의 점선으로 둘러싼 부분, 즉 디바이스 0, 1, 2, 3를 하나의 그룹으로서 일괄하여 데이터를 송부하는 처리를 실행한다. 이러한 그룹은 도 4의 트리 중에 복수개 존재한다.

또, 노드 키, 리프 키는, 임의의 하나의 키 관리 센터에 의해 통합하여 관리하여도 되고, 각 그룹에 대한 다양한 데이터 송수신을 행하는 프로바이더, 결제 기관 등에 의해 그룹으로 관리하는 구성으로 하여도 된다. 이들 노드 키, 리프 키는 예를 들면 키의 누설 등의 경우에 갱신 처리가 실행되며, 이 갱신 처리는 키 관리 센터, 프로바이더, 결제 기관 등이 실행한다.

이 트리 구조에서, 도 4로부터 명백한 바와 같이, 하나의 그룹에 포함되는 4개의 디바이스 0, 1, 2, 3는 노드 키로서 공통의 키 K00, K0, KR를 보유한다. 이 노드 키 공유 구성을 이용함으로써, 예를 들면 공통의 마스터 키를 디바이스 0, 1, 2, 3에만 제공하는 것이 가능해진다. 예를 들면, 공통으로 보유하는 노드 키 K00 자체를 마스터 키로서 설정하면, 새로운 키 송부를 실행하지 않고 디바이스 0, 1, 2, 3만이 공통적인 마스터 키의 설정이 가능하다. 또한, 새로운 마스터 키 Kmaster를 노드 키 K00으로 암호화한 값 Enc(K00, Kmaster)를, 네트워크를 통해 혹은 기록 매체에 저장하여 디바이스 0, 1, 2, 3에 배포하면, 디바이스 0, 1, 2, 3만이 각각의 디바이스에서 보유하는 공유 노드 키 K00을 이용하여 암호 Enc(K00, Kmaster)를 풀어 마스터 키: Kmaster를 얻는 것이 가능해진다. 또, Enc(Ka, Kb)는 Kb를 Ka에 의해 암호화한 데이터인 것을 나타낸다.

또한, 임의의 시점 t 에서, 디바이스 3이 소유하는 키: $K0011$, $K001$, $K00$, $K0$, $KR0$ 공격자(해커)에 의해 해독되어 노출된 것이 발각된 경우, 그 이후, 시스템(디바이스 0, 1, 2, 3의 그룹)으로 송수신되는 데이터를 보호하기 위해, 디바이스 3을 시스템으로부터 분리할 필요가 있다. 그것을 위해서는, 노드 키: $K001$, $K00$, $K0$, KR 을 각각 새로운 키 $K(t)001$, $K(t)00$, $K(t)0$, $K(t)R$ 로 갱신하고, 디바이스 0, 1, 2에 그 갱신 키를 전달할 필요가 있다. 여기서, $K(t)aaa$ 는, 키 $Kaaa$ 의 세대(Generation): t 의 갱신 키인 것을 나타낸다.

갱신 키의 배포 처리에 대하여 설명한다. 키의 갱신은, 예를 들면, 도 5A에 나타낸다. 키 갱신 블록(KRB: Key Renewal Block)이라 불리우는 블록 데이터에 의해 구성되는 테이블을 예를 들면 네트워크, 혹은 기록 매체에 저장하여 디바이스 0, 1, 2에 공급함으로써 실행된다.

도 5A에 도시한 키 갱신 블록(KRB)에는, 노드 키의 갱신이 필요한 디바이스만이 갱신 가능한 데이터 구성을 갖는 블록 데이터로서 구성된다. 도 5A 및 도 5B의 예는, 도 4에 도시한 트리 구조 중의 디바이스 0, 1, 2에서, 세대 t 의 갱신 노드 키를 배포하는 것을 목적으로서 형성된 블록 데이터이다. 도 4로부터 명백한 바와 같이, 디바이스 0, 디바이스 1은 갱신 노드 키로서 $K(t)00$, $K(t)0$, $K(t)R$ 이 필요하며, 디바이스 2는 갱신 노드 키로서 $K(t)001$, $K(t)00$, $K(t)0$, $K(t)R$ 이 필요하다.

도 5A의 KRB에 도시된 바와 같이 KRB에는 복수의 암호화 키가 포함된다. 최하단의 암호화 키는 $Enc(K0010, K(t)001)$ 이다. 이것은 디바이스 2가 갖는 리프 키 $K0010$ 에 의해 암호화된 갱신 노드 키 $K(t)001$ 이며, 디바이스 2는 자신이 갖는 리프 키에 의해 이 암호화 키를 복호하여, $K(t)001$ 을 얻을 수 있다. 또한, 복호에 의해 얻은 $K(t)001$ 을 이용하여, 도 5A의 하단으로부터 2단계의 암호화 키 $Enc(K(t)001, K(t)00)$ 가 복호 가능해지고, 갱신 노드 키 $K(t)00$ 을 얻을 수 있다. 이하 순차적으로 도 5A의 상단으로부터 2단계의 암호화 키 $Enc(K(t)00, K(t)0)$ 를 복호하고, 갱신 노드 키 $K(t)0$, 도 5A의 상단으로부터 1단계의 암호화 키 $Enc(K(t)0, K(t)R)$ 를 복호하여 $K(t)R$ 을 얻는다. 한편, 디바이스 0, 1은 노드 키 $K000$ 은 갱신하는 대상에 포함되지 않고, 갱신 노드 키로서 필요한 것은 $K(t)00$, $K(t)0$, $K(t)R$ 이다. 디바이스 0, 1은 도 5A의 상단으로부터 3단계의 암호화 키 $Enc(K000, K(t)00)$ 를 복호하여 $K(t)00$ 을 취득하고, 이하, 도 5A의 상단으로부터 2단계의 암호화 키 $Enc(K(t)00, K(t)0)$ 를 복호하고, 갱신 노드 키 $K(t)0$, 도 5A의 상단으로부터 1단계의 암호화 키 $Enc(K(t)0, K(t)R)$ 를 복호하여 $K(t)R$ 을 얻는다. 이와 같이 하여, 디바이스 0, 1, 2는 갱신한 키 $K(t)R$ 을 얻는 것이 가능하게 된다. 또, 도 5A의 인덱스는 복호 키로서 사용하는 노드 키, 리프 키의 절대 번지를 나타낸다.

도 4에 도시한 트리 구조의 상위단의 노드 키: $K(t)0$, $K(t)R$ 의 갱신이 불필요하고, 노드 키 $K00$ 만의 갱신 처리가 필요한 경우에는, 도 5B의 키 갱신 블록(KRB)을 이용함으로써, 갱신 노드 키 $K(t)00$ 을 디바이스 0, 1, 2에 배포할 수 있다.

도 5B에 도시한 KRB는, 예를 들면 특정한 그룹의 정보 기억 장치에서 공유하는 새로운 마스터 키, 정보 기억 장치 고유의 디바이스 키 혹은 기록 매체에 고유의 미디어 키를 배포하는 경우에 이용 가능하다. 구체예로서, 도 4에 점선으로 나타내는 그룹 내의 디바이스 0, 1, 2, 3이 있는 기록 매체를 이용하고 있으며, 새로운 공통의 마스터 키 $K(t)master$ 가 필요하다고 한다. 이 때, 디바이스 0, 1, 2, 3의 공통의 노드 키 $K00$ 을 갱신한 $K(t)00$ 을 이용하여 새로운 공통의 갱신 마스터 키: $K(t)master$ 를 암호화한 데이터 $Enc(K(t), K(t)master)$ 를 도 5B에 도시한 KRB와 함께 배포한다. 이 배포에 의해 디바이스 4 등, 그 밖의 그룹의 기기에서는 복호되지 않은 데이터로서의 배포가 가능해진다. 미디어 키에 대해서도 마찬가지이다.

즉, 디바이스 0, 1, 2, 3은 KRB를 처리하여 얻은 $K(t)00$ 을 이용하여 상기 암호문을 복호하면, t 시점에서의 마스터 키: $K(t)master$ 나 미디어 키: $K(t)media$ 를 얻는 것이 가능해진다.

이상의 진술을 정리해 보면, 각 디바이스에서의 처리는 이하와 같이 설명할 수 있다.

1. 각 디바이스는 각각, KRB의 인덱스(index)부를 보고, KRB로 보내지는 트리 구조를 알 수 있다.
2. KRB에 의해 갱신되어 있지 않은 (살아 있는) 노드 키 중 최상위의 키(이 예에서는, 디바이스 0, 1이면 $K000$, 디바이스 2이면 $K0010$)를 이용하여 암호문을 푸는 것에 의해, 그 노드의 모(母) 노드가 갱신된 노드 키를 얻는다.
3. 갱신된 노드 키를 이용하여 암호문을 푸는 것에 의해, 그 노드의 모 노드가 갱신된 노드 키를 얻는다.
4. 이것을 반복하여, KRB의 최상위의 노드가 갱신된 노드 키를 얻는다.

또, KRB의 세대는, 그 KRB의 버전을 나타내고, 예를 들면 새로운 것은 값을 크게 해 두는 등, 그 값을 비교함으로써 KRB의 신규(新舊) 비교를 행할 수 있도록 되어 있다. 또한, $K(t)0$, $K(t)R$ 의 갱신이 불필요한 경우에는, 도 5B의 KRB를 이용함으로써, $K(t)00$ 을 디바이스 0, 1, 2로 공유할 수 있다. 즉, 디바이스 0, 1, 2, 3이 임의의 기록 매체를 이용하는 하나의 그룹을 형성할 때, $K(t)00$ 을 이용하여 전송한 미디어 키를 이용하여 기록 데이터를 암호화함으로써, 디바이스 4 등, 그 밖의 그룹의 기기로부터는 액세스되지 않은 데이터로 하는 것이 가능해진다. 구체적으로, 예를 들면, 도 5B를 이용하여 디바이스 0, 1, 2는 $K(t)00$ 을 공유하지만, 이 KRB를 저장한 기록 매체에, t 시점에서의 미디어 키 $K(t)media$ 를 암호화하여 저장해 둔다. 디바이스 0, 1, 2는 KRB를 처리하여 얻은 $K(t)00$ 을 이용하여 상기 암호문을 복호하고, t 시점에서의 미디어 키 $K(t)media$ 를 얻는다.

도 6에, 본 출원인의 특허 출원인 특원평2000-105322에서 제안한 t 시점에서의 미디어 키 $K(t)media$ 를 얻는 처리예로서, $K(t)00$ 을 이용하여 새로운 공통의 미디어 키: $K(t)media$ 를 암호화한 데이터 $Enc(K(t)00, K(t)media)$ 와 도 5B에 도시한 KRB를 기록 매체를 통해 수령한 디바이스 2의 처리를 나타낸다.

도 4에 도시한 바와 같이, 어떤 기록 재생 시스템에는, 점선으로 둘러싸인, 디바이스 0, 1, 2, 3의 4개의 장치가 포함되도록 한다. 도 6은 디바이스 3이 리브크되었을 때, 기록 매체마다 팔당되는 미디어 키를 사용하는 경우에, 기록 재생 장치(디바이스 2)가 기록 매체 상의 콘텐츠를 암호화 혹은 복호하기 위해 필요한 미디어 키를, 기록 매체에 저장되어 있는 KRB와 기록 재생 장치가 기억하는 디바이스 키를 이용하여

구할 때의 처리를 나타내고 있다.

디바이스 2의 메모리에는, 자신에게만 할당된 리프 키 K0010과, 그 곳으로부터 트리의 루트까지의 각 노드 001, 00, 0, R의 노드 키가 각각, K001, K00, K0, KR이 안전하게 저장되어 있다. 디바이스 2는 도 6의 기록 매체에 저장되어 있는 KRB 중, 인덱스(index)가 0010의 암호문을 자신이 갖는 리프 키가 K0010으로 복호하여 노드 001의 노드 키 K(t)001을 계산하고, 다음에 그것을 이용하여 인덱스(index)가 001의 암호문을 복호하여 노드 00의 노드 키 K(t)00을 계산하고, 마지막으로 그것을 이용하여 암호문을 복호하여 미디어 키 K(t)media를 계산할 필요가 있다. 이 계산-횟수는 리프로부터 미디어 키를 암호화하는 노드까지의 길이가 깊게 되는 데 비례하여 증가한다. 즉, 많은 기록 재생 장치가 존재하는 큰 시스템에서는 많은 계산이 필요해진다. 이와 같이 하여 계산되고, 취득된 미디어 키를 이용한 데이터의 암호화 처리, 복호 처리 양태에 대하여 이하, 설명한다.

도 7의 처리 블록도에 따라서, 암호 처리 수단(150)이 실행하는 데이터의 암호화 처리 및 기록 매체에 대한 기록 처리의 일례에 대하여 설명한다.

기록 재생 장치(700)는 자신이 상술한 KRB에 기초하는 산출 처리에 의해 미디어 키를 취득한다.

다음에, 기록 재생 장치(700)는 예를 들면 광 디스크인 기록 매체(702)에 식별 정보로서의 디스크 ID(Disc ID)가 이미 기록되어 있는지의 여부를 검사한다. 기록되어 있으면, 디스크 ID(Disc ID)를 판독하고, 기록되어 있지 않으면, 암호 처리 수단(150)에서 랜덤하게, 혹은 사전에 정해진 예를 들면 난수 발생 등의 방법으로 디스크 ID(Disc ID, 1701)를 생성하고, 디스크에 기록한다. 디스크 ID(Disc ID)는 그 디스크에 하나 있으면 되므로, 리드의 영역 등에 저장하는 것도 가능하다.

기록 재생기(700)는, 다음에 미디어 키(701)와 디스크 ID를 이용하여, 디스크 고유 키(Disc Unique Key)를 생성한다. 디스크 고유 키(Disc Unique Key)의 구체적인 생성 방법으로서, 도 8에 도시한 바와 같이, 블록 암호 함수를 이용한 해시 함수에 미디어 키와 디스크 ID(Disc ID)를 입력하여 얻어진 결과를 이용하는 예 1의 방법이나, FIPS(Federal Information Processing Standards Publications) 180-1로 정해져 있는 해시 함수 SHA-1에, 미디어 키와 디스크 ID(Disc ID)와의 비트 연결에 의해 생성되는 데이터를 입력하고, 그 160비트의 출력으로부터 필요한 데이터 길이만을 디스크 고유 키(Disc Unique Key)로서 사용하는 예 2의 방법을 적용할 수 있다.

다음에, 기록매체의 고유 키인 타이틀 키(Title Key)를 암호 처리 수단(150: 도 1 참조)에서 랜덤하게, 혹은 사전에 정해진 예를 들면 난수 발생 등의 방법으로 생성하여, 디스크(702)에 기록한다.

다음에, 디스크 고유 키(Disc Unique Key)와 타이틀 키(Title Key)와, 디바이스 ID, 혹은, 디스크 고유 키(Disc Unique Key)와 타이틀 키(Title Key)와, 디바이스 고유 키 중 어느 하나의 조합으로부터, 타이틀 고유 키(Title Unique Key)를 생성한다.

이 타이틀 고유 키(Title Unique Key) 생성의 구체적인 방법은, 도 9에 도시한 바와 같이, 블록 암호 함수를 이용한 해시 함수에 타이틀 키(Title Key)와 디스크 고유 키(Disc Unique Key)와, 디바이스 ID(재생 기기 제한을 하지 않는 경우) 혹은 디바이스 고유 키(재생 기기 제한을 하는 경우)를 입력하여 얻어진 결과를 이용하는 예 1의 방법이나, FIPS 180-1로 정해져 있는 해시 함수 SHA-1에, 미디어 키와 디스크 ID(Disc ID)와 디바이스 ID(재생 기기 제한을 하지 않는 경우) 혹은 디바이스 고유 키(재생 기기 제한을 하는 경우)와의 비트 연결에 의해 생성되는 데이터를 입력하고, 그 160비트의 출력으로부터 필요한 데이터 길이만을 타이틀 고유 키(Title Unique Key)로서 사용하는 예 2의 방법을 적용할 수 있다. 또, 재생 기기 제한이란, 기록 매체에 저장된 콘텐츠 데이터를 제한된 특정한 재생 기기에서만 재생 가능하게 하는 것을 의미한다.

또, 상기한 설명에서는, 미디어 키와 디스크 ID(Disc ID)로부터 디스크 고유 키(Disc Unique Key)를 생성하고, 이것과 타이틀 키(Title Key)와 디바이스 ID, 혹은 타이틀 키(Title Key)와 디바이스 고유 키로부터 타이틀 고유 키(Title Unique Key)를 각각 생성하도록 하고 있지만, 디스크 고유 키(Disc Unique Key)를 불필요로 하여 미디어 키와 디스크 ID(Disc ID)와 타이틀 키(Title Key)와, 디바이스 ID 혹은 디바이스 고유 키로부터 직접 타이틀 고유 키(Title Unique Key)를 생성하여도 되며, 또한, 타이틀 키(Title Key)를 이용하지 않고서, 미디어 키(Master Key)와 디스크 ID(Disc ID)와, 디바이스 ID 혹은 디바이스 고유 키로부터 타이틀 고유 키(Title Unique Key) 상당의 키를 생성하여도 된다.

또한, 도 7을 참조하여, 그 후의 처리를 설명한다. 피암호화 데이터로서 입력되는 블록 데이터의 선두의 제1~4 바이트가 분리되어 출력되는 블록 시드(Block Seed)와, 앞에서 생성된 타이틀 고유 키(Title Unique Key)로부터, 그 블록의 데이터를 암호화하는 키인 블록 키(Block Key)가 생성된다.

블록 키(Block Key)의 생성 방법의 예를 도 10에 도시한다. 도 10에서는, 어느 것이나 32비트의 블록 시드(Block Seed)와, 64비트의 타이틀 고유 키(Title Unique Key)로부터, 64비트의 블록 키(Block Key)를 생성하는 예를 7가지 나타내고 있다.

상단에 나타낸 예 1은 키 길이 64비트, 임플렉이 각각 64비트의 암호 함수를 사용하고 있다. 타이틀 고유 키(Title Unique Key)를 이 암호 함수의 키로 하여, 블록 시드(Block Seed)와 32비트의 상수(constant)를 연결한 값을 입력하여 암호화한 결과를 블록 키(Block Key)로 하고 있다.

예 2는 FIPS 180-1의 해시 함수 SHA-1을 이용한 예이다. 타이틀 고유 키(Title Unique Key)와 블록 시드(Block Seed)를 연결한 값을 SHA-1에 입력하고, 그 160비트의 출력을, 예를 들면 하위 64비트만 사용하는 등, 64비트로 축약한 것을 블록 키(Block Key)로 하고 있다.

또, 상기에서는 디스크 고유 키(Disc Unique Key), 타이틀 고유 키(Title Unique Key), 블록 키(Block Key)를 각각 생성하는 예를 설명하였지만, 예를 들면, 디스크 고유 키(Disc Unique Key)와 타이틀 고유 키(Title Unique Key)의 생성을 실행하지 않고, 블록마다 미디어 키와 디스크 ID(Disc ID)와 타이틀 키(Title Key)와 블록 시드(Block Seed)와, 디바이스 ID, 혹은 디바이스 고유 키를 이용하여 블록 키(Block Key)를 생성하여도 된다.

블록 키가 생성되면, 생성된 블록 키(Block Key)를 이용하여 블록 데이터를 암호화한다. 도 7의 하단에 도시한 바와 같이, 블록 시드(Block Seed)를 포함한 블록 데이터의 선두의 제1~ m 바이트(예를 들면 $m=8$ 바이트)는 분리(셀렉터 1608)되어 암호화 대상으로 하지 않고, $m+1$ 바이트째로부터 최종 데이터까지를 암호화한다. 또, 암호화되지 않은 m 바이트 중에는 블록 시드로서의 제1~4 바이트도 포함된다. 셀렉터에 의해 분리된 제11 바이트 이후의 데이터는, 암호 처리 수단(150)에 사전에 설정된 암호화 알고리즘에 따라 암호화된다. 암호화 알고리즘으로서, 예를 들면 FIPS 46-2로 규정되는 DES(Data Encryption Standard)를 이용할 수 있다.

이상의 처리에 의해, 콘텐츠는 블록 단위로 세대 관리된 미디어 키, 블록 시드 등에 기초하여 생성되는 블록으로 암호화가 실시되어 기록 매체에 저장된다.

도 11은 기록 매체에 저장된 암호화 콘텐츠 데이터의 복호 및 재생 처리를 설명하는 블록도를 나타낸다.

재생 처리에서는, 도 7~도 10을 참조하며 설명한 암호화 및 기록 처리와 마찬가지로 미디어 키와 디스크 10로부터 디스크 고유 키를 생성하고, 디스크 고유 키와, 타이틀 키로부터 타이틀 고유 키를 생성하고, 또한 타이틀 키와 기록 매체로부터 판독되는 블록 시드로부터 블록 키를 생성하여, 블록 키를 복호 키로서 이용하고, 기록 매체(702)로부터 판독되는 블록 단위의 암호화 데이터의 복호 처리를 실행한다.

상술된 바와 같이, 콘텐츠 데이터의 기록 매체에 대한 기록 시의 암호화 처리, 및 기록 매체로부터의 재생 시의 복호 처리에서는, KRB에 기초하여 미디어 키를 산출하고, 그 후 산출한 미디어 키와 다른 식별자 등에 기초하여 콘텐츠의 암호화 처리용의 키, 또는 복호 처리용의 키를 생성한다.

또, 상술한 예에서는, 미디어 키를 이용하여 콘텐츠 데이터의 암호화 처리, 및 복호 처리에 이용하는 키를 생성하는 구성을 설명하였지만, 미디어 키가 아니라, 복수의 기록 재생 장치에 공통의 마스터 키, 혹은 기록 재생기 고유의 디바이스 키를 KRB로부터 취득하고, 이에 기초하여 콘텐츠 데이터의 암호화 처리, 및 복호 처리에 이용하는 키를 생성하는 구성으로 하여도 된다. 또한, KRB로부터 얻어 되는 미디어 키, 마스터 키, 혹은 디바이스 키 자체를 콘텐츠 데이터의 암호화 처리, 및 복호 처리에 이용하는 키로서 적용하는 것도 가능하다.

상술한 바와 같이, 키 갱신 블록(KRB)을 이용함으로써, 정당한 라이선스를 받은 디바이스에 대해서만 안전하게 갱신 키를 제공하고, 제공한 키에 의해 기록 매체에 대한 콘텐츠 암호화 처리, 또는 기록 매체로부터 판독한 콘텐츠의 복호 처리에 이용하는 키의 생성이 가능해진다. 상술한 구성에서는, 예를 들면 하나의 기록 매체에 단 하나의 키 갱신 블록(KRB)을 저장하고, 이것을 이용하여 갱신 키의 취득을 행하는 예를 설명하였지만, 또한, 복수의 키 갱신 블록(KRB)을 저장한 구성 예에 대하여 이하 설명한다. 이 경우, 후단에서 상세히 설명하지만, 기록 매체 상의 기록 암호화 콘텐츠 데이터의 각각을, 복수의 키 갱신 블록(KRB) 중 어느 하나의 KRB로부터 생성되는 미디어 키를 이용하여 암호화된 것인지를 판별할 수 있는 정보를 갖는 구성으로 한다.

또한, 기록 매체만이 아니라, 기록 재생 장치의 메모리에 KRB를 저장하는 구성으로 하여도 된다. 기록 재생 장치의 키 갱신 블록(KRB) 저장용의 기억 수단은, 재기입 가능한 구성이며, 기록 재생 장치는 기록 매체에 액세스 시에, 예를 들면, 기록 매체가 기록 재생 장치에 장착될 때에, 기록 매체 상의 KRB를 검색하고, 그 중에서 가장 버전이 새로운 것이, 자신이 저장하는 것보다도 새로운 것이면, 이것을 이용하여 자신이 저장하는 KRB를 갱신한다.

도 12에 키 갱신 블록(KRB)의 포맷예를 나타낸다. 버전(1201)은 키 갱신 블록의 버전을 나타내는 식별자이다. 길이는, 키 갱신 블록(KRB)의 배포처의 디바이스에 대한 계층 트리의 계층 수를 나타낸다. 데이터 포인터(1203)는 키 갱신 블록(KRB) 중의 데이터부의 위치를 나타내는 포인터이며, 태그 포인터(1204)는 태그부의 위치, 서명 포인터(1205)는 서명의 위치를 나타내는 포인터이다. 데이터부(1206)는, 예를 들면 갱신하는 노드 키를 암호화한 데이터를 저장한다.

태그부(1207)는 데이터부에 저장된 암호화된 노드 키, 리프 키의 위치 관계를 나타내는 태그이다. 이 태그의 부여 룰에 대하여 도 13을 참조하여 설명한다. 도 13에서는, 데이터로서 앞의 도 5A에서 설명한 키 갱신 블록(KRB)을 송부하는 예를 나타내고 있다. 이 때의 데이터는, 도 13의 우측의 표에 나타난 바와 같다. 이 때의 암호화 키에 포함되는 톰 노드의 어드레스를 톰 노드 어드레스라고 한다. 이 경우에는, 루트 키의 갱신 키 $K(t)_{ROI}$ 포함되어 있으므로, 톰 노드 어드레스는 KR로 된다.

암호화 키의 최상단의 데이터 $Enc(K(t)_0, K(t)_R)$ 는, 도 13의 좌측의 계층 트리에 나타내는 위치에 있다. 여기서, 다음의 데이터는 $Enc(K(t)_0, K(t)_0)$ 이고, 트리 상에서는 이전의 데이터에 대하여 좌측 아래의 위치에 있다. 태그는, 그 데이터에 대하여 하위 계층의 데이터가 있는 경우에는 0, 없는 경우에는 1로 설정된다. 태그는 {좌측(L) 태그, 우측(R) 태그}로서 표현된다. 최상단의 데이터 $Enc(K(t)_0, K(t)_R)$ 의 좌측에는 데이터가 있으므로, L 태그=0, 우측에는 데이터가 없기 때문에, R 태그=1로 된다. 이하, 모든 데이터에 태그가 설정되고, 도 13의 하단에 나타내는 데이터 열, 및 태그 열이 구성된다.

도 12로 되돌아가, KRB 포맷에 대하여 더욱 설명한다. 서명(Signature)은, 키 갱신 블록(KRB)을 발행한 예를 들면 키 관리 센터, 콘텐츠 프로바이더, 결제 기관 등이 실행하는 전자 서명 KRB를 수령한 디바이스는 서명 검증에 의해 정당한 키 갱신 블록(KRB) 발행자가 발행한 키 갱신 블록(KRB)인 것을 확인한다.

다음에, 키 갱신 블록(KRB)의 갱신 처리에 대한 제1 실시예에 대하여 설명한다. 기록 매체에 복수의 키 갱신 블록(KRB)을 저장하는 구성, 또한, 기록 재생 장치의 메모리에 최신의 KRB를 저장하는 처리, 즉, 기록 재생 장치측에 저장한 키 갱신 블록(KRB)을 갱신하는 처리에 대하여, 도 14의 (A) 및 (B)의 개념도 및 도 15의 흐름도를 참조하여 설명한다.

도 14 중 상단에 도시한 (A)는 기록 재생 기기에 기록 매체가 장착되는 이전의 상태이며, 기록 재생 장치(1410)에 하나의 키 갱신 블록(KRB: 1411)이 저장되고, 기록 매체(1420)에는 2개의 키 갱신 블록(KRB: 1421, 1422)이 저장되어 있는 상태를 나타내고 있다.

기록 재생 장치(1410)에 저장된 KRB는, 버전(T1)의 키 갱신 블록(KRB: 1411)이고, 기록 매체(1420)에 저장된 KRB는 버전(T1)의 키 갱신 블록(KRB: 1421), 및 버전(T2)의 키 갱신 블록(KRB: 1422)이다. 여기서 버전(T2)은 버전(T1)보다 새로운 것으로 한다.

또한, 기록 매체(1420)에는, 버전(T1)의 키 갱신 블록(KRB)으로부터 생성되는 미디어 키를 이용하여 암호화된 콘텐츠(1431)와, 버전(T2)의 키 갱신 블록(KRB)으로부터 생성되는 미디어 키를 이용하여 암호화된 콘텐츠(1432)가 저장되어 있다.

기록 매체(1420)가 기록 재생 장치(1410)에 장착될 때, 기록 재생 장치는 도 15의 흐름도에 따라, 자신이 저장하는 키 갱신 블록(KRB)의 갱신 처리를 행한다.

도 15의 단계 S1501에서, 기록 재생 장치(1410)는 기록 매체(1420)에 저장되어 있는 모든 키 갱신 블록(KRB)의 세대 정보(Generation)인 버전을 판독하고, 그 중에서 최신의 것을 찾아낸다. 도 14의 (A)에 도시한 예에서는, 버전(T2)의 키 갱신 블록(KRB: 1422)이 최신이다.

단계 S1502에서, 기록 재생 장치(1410)는 기록 재생 장치 내의 메모리(예를 들면 도 1의 메모리(180))에 저장되어 있는 키 갱신 블록(KRB)과, 단계 S1501에서 검출한 기록 매체(1420) 상의 최신 KRB, 즉 버전(T2)의 키 갱신 블록(KRB: 1422)과의 신구를 비교한다.

이 비교에서, 기록 매체 상에서 검출한 KRB 쪽이 새로우면 단계 S1503으로 진행하고, 그렇지 않으면 단계 S1503, S1504를 스킵하여 처리를 종료한다.

도 14의 (A)의 예에서는, 기록 재생 장치(1410)가 저장하고 있는 것은 버전(T1)의 키 갱신 블록(KRB: 1411)이며, 이보다 버전(T2)의 키 갱신 블록(KRB: 1422) 쪽이 새롭기 때문에, 단계 S1503으로 진행한다.

단계 S1503에서는, 기록 재생 장치(1410)가 보유하고 있는 리프 키, 노드 키를 이용하여 갱신 예정의 최신의 KRB가 복호 가능한지의 여부를 판정한다. 즉, 앞의 도 4, 5, 6 등에서 설명한 바와 같이, 자기가 갖는 리프 키, 또는 노드 키에 의해 키 갱신 블록(KRB)을 순차 복호하고, 세대가 갱신된 세대 정보, 즉 신 버전의 노드 키, 예를 들면 K(t)00, 또는 K(t)00이 취득 가능한지의 여부를 판정한다. 이 판정 처리는, 예를 들면 도 5에 도시한 키 갱신 블록(KRB)에서, 어느 하나의 인덱스에 자기가 갖는 리프 키, 노드 키를 그대로 적용하여 복호 가능한 암호화 키가 저장되어 있는지의 여부를 판정함으로써 행해진다.

단계 S1503에서, 기록 재생 장치(1410)가 보유하고 있는 리프 키, 노드 키를 이용하여 갱신 예정의 최신의 KRB가 복호 가능하다고 판정된 경우에는, 단계 S1504로 진행한다. 복호 불가능하고 판정된 경우에는, 단계 S1504를 스킵하여 처리를 종료한다.

단계 S1504에서는, 단계 S1501에서 검출한 기록 매체(1420)에 저장된 최신의 KRB를 이용하여, 기록 재생 장치(1410)가 메모리에 저장하고 있는 버전(T1)의 키 갱신 블록(KRB: 1411)을 갱신한다. 이 결과, 도 14(B)에 도시한 바와 같이, 기록 재생 장치(1410)에 저장되는 KRB가 버전(T2)의 키 갱신 블록(KRB: 1412)에 갱신된다.

다음에, 도 16A, 도 16B 및 도 17의 흐름도를 이용하여, 도 1에 도시한 기록 재생 장치가 기록 매체에 콘텐츠 데이터를 기록하는 처리를 설명한다.

도 16의 상단에 도시한 도 16A의 기록 재생 장치(1610)는, 버전(T2)의 키 갱신 블록(KRB: 1611)을 저장하고 있어, 콘텐츠를 암호화하여 기록 매체(1620)에 기록하려고 한다.

기록 매체(1620)에는, 버전(T1)의 키 갱신 블록(KRB: 1621)이 기록되어 있으며, 이 키 갱신 블록(KRB: 1621)으로부터 생성된 미디어 키에 기초하여 암호화된 콘텐츠(1631)가 기록되어 있다.

도 17은, 기록 재생 장치가 기록 매체에 대하여 콘텐츠 데이터를 기록할 때의 처리 흐름을 나타낸 것이다. 도 17의 흐름의 각 단계에 대하여 설명한다.

단계 S1701에서, 기록 재생 장치(1610)는 자신이 저장하는 버전(T2)의 키 갱신 블록(KRB: 1611)으로부터 미디어 키를 생성한다.

기록 재생 장치(1610)는, 이 기록 매체(1620)가 장착되었을 때, 앞에서 설명한 도 15의 키 갱신 블록(KRB) 갱신 처리를 행하고 있으며, 장치의 메모리 내에는 장치 및 매체 상의 키 갱신 블록(KRB) 중의 최신의 것. 여기서는 버전 T2의 키 갱신 블록(KRB)이 저장되어 있다.

단계 S1702에서, 이 미디어 키에 기초하여 콘텐츠 데이터를 암호화한다. 이 암호화 처리는, 예를 들면 앞의 도 7을 이용하여 설명한 방법에 따라 실행된다. 그 후, 암호화 콘텐츠 데이터는 기록 매체(1620)에 기록된다. 또, 암호화 콘텐츠의 기록 매체(1620)에 대한 저장 처리 시에, 그 콘텐츠 암호화에 이용한 미디어 키를 취득한 키 갱신 블록(KRB)의 세대 정보로서의 버전, 이 경우에는, 키 갱신 블록(KRB: 1611)의 버전(T2)을 암호화 콘텐츠에 대응하여 기록 매체(1620)에 기록한다. 이, 키 갱신 블록(KRB)의 세대 정보로서의 버전 정보는, 구체적으로는 예를 들면, 도 7에 도시한 타이틀 키 등의 콘텐츠의 부가 정보와 마찬가지로, 콘텐츠 데이터와 관련된 관리 파일로서 구성되는 데이터 관리 파일 중에 기록되어 기록 매체(1620)에 저장된다.

다음에, 단계 S1703에서, 기록 재생 장치(1610)는 미디어 키를 생성하는 데 이용한 것과 동일한 버전의 키 갱신 블록(KRB)이 기록 매체(1620)에 저장되어 있는지의 여부를 검사한다. 만일 기록 매체(1620)에 저장되어 있으면, 단계 S1704를 스킵하여 처리를 종료하고, 저장되어 있지 않으면, S1704로 진행한다.

단계 S1704에서는, 기록 재생 장치(1610)는 기록 매체(1620)에, 미디어 키를 생성하는 데 이용한 것과 동일한 버전의 키 갱신 블록(KRB), 이 경우에는, 버전(T2)의 키 갱신 블록(KRB)을 기록하여, 콘텐츠 데이터의 기록 처리를 종료한다. 이상의 처리에 의해, 도 16B에서 도시한 바와 같이, 기록 매체(1620)에는, 이용 가능한 최신의 KRB로부터 취득되는 미디어 키를 이용하여 암호화한 암호화 콘텐츠 데이터, 및 콘텐츠 암호 처리에 필요해지는 미디어 키를 얻기 위해 필요해지는 최신의 키 갱신 블록(KRB)을 기록 매체(1620)에 저장된다.

0)에 기록할 수 있다.

다음에, 상기한 바와 같이 하여, 이용 가능한 최신의 키 갱신 블록(KRB)에 기초하여 얻어지는 키를 이용 하여 암호화되고, 기록된 콘텐츠 데이터를, 기록 매체로부터 기록 재생 장치가 판독하는 처리를, 도 18 의 흐름도를 이용하여 설명한다.

단계 S1801에서, 기록 재생 장치는, 재생하는 콘텐츠 데이터를 암호화한 미디어 키를 생성하는 키 갱신 블록(KRB)의 세대 정보로서의 버전을 판독한다. 기록 매체 상의 각 콘텐츠 데이터에 대응하는 키 갱신 블록(KRB)의 세대 정보로서의 버전은, 예를 들면, 전송한 데이터 관리 파일에 기록되어 있다.

단계 S1802에서, 기록 재생 장치는 기록 매체 상에 저장되어 있는 1 이상의 키 갱신 블록(KRB) 중, 단계 S1801에서 판독한 세대 정보로서의 버전과 동일한 버전을 갖는 것을 검출하고, 그 키 갱신 블록(KRB)을 복호 처리하여, 미디어 키를 생성한다.

다음에, 단계 S1803에서, 기록 재생 장치는 기록 매체로부터 콘텐츠 데이터를 판독하고, S1802에서 생성 한 미디어 키에 기초하여 이것을 복호하여 사용한다. 이상의 처리에 의해, 기록 매체에 저장된 콘텐츠 데 이터를 재생할 수 있다.

이와 같이, 본 발명의 정보 기록 재생 장치에서는, 복수의 다른 세대, 즉, 버전을 갖는 키 갱신 블록(KRB)을 저장한 기록 매체로부터 최신의 키 갱신 블록(KRB)을 추출하여, 기록 재생 장치 내의 메모리에 저장 하고, 또한, 기록 매체에 대한 콘텐츠 저장 처리에서는, 기록 재생 장치 내의 메모리에 저장된 KRB, 및 기록 매체에 저장된 복수의 KRB 중으로부터, 이용 가능한 최신의 키 갱신 블록(KRB)을 검출하여, 그 최신 KRB로부터 암호 처리용의 키, 예를 들면, 미디어 키를 취득하여, 취득한 최신의 미디어 키를 이용하여 콘 텐츠의 암호화 처리를 실행하여, 기록 매체에 저장하고, 콘텐츠의 암호화에 이용한 미디어 키를 취득한 키 갱신 블록(KRB)을 새롭게 기록 매체에 저장하는 구성으로 하였다.

이와 같이 복수의 버전의 KRB를 기록 매체에 저장 가능하게 함과 함께, 다른 KRB로부터 취득한 미디어 키 로 암호화한 콘텐츠를 기록 매체에 저장 가능한 구성으로 하고, 콘텐츠를 기록 매체에 새롭게 기록할 때 에는, 그 시점에서 기록 재생 장치와 기록 매체가 보유하는 최신의 KRB에 기초하여 산출되는 미디어 키를 이용하여, 콘텐츠의 암호화가 이루어지기 때문에, 예를 들면 기록 매체의 제조 시에, 콘텐츠 암호화에 이용 된 오래된 버전의 KRB가 기록 매체에 저장되었다고 해도, 앞의 도 4, 도 5를 참조하여 설명한 바와 같이, 새롭게 키 관리 센터에서 프로바이더, 결제 기관 등이 실행하는 키 갱신 처리에 의해 발행된 새로운 버전 의 KRB를 결정된 기기를 리브로크하여, 발행함으로써, 그 후, 기록 매체에 저장되는 암호화 콘텐츠는, 정當 한 기기만이 취득 가능한 새로운 버전의 KRB로부터 취득되는 미디어 키에 기초하여 암호화되게 되므로, 리브로크된 기기에서의 복호, 재생을 배제하는 것이 가능해진다.

또, 상술한 실시예의 설명에서는, 미디어 키를 암호 처리용 키로서 이용하는 예를 중심으로 하여 설명하 였지만, KRB에 의해 갱신되는 암호 처리용 키는, 예를 들면 복수의 정보 기록 장치에 공통인 마스터 키, 정보 기록 재생 장치에 고유의 디바이스 키로도 되고, 상기한 KRB에 의한 키 갱신은, 마스터 키, 디바이스 키에 대해서도 미디어 키와 마찬가지로 처리가 적용 가능하다.

또한, 상술한 실시예에서는, 기록 매체(1620)가 기록 재생 장치(1610)에 장착된 시점에서 키 갱신 블록 (KRB)의 갱신 처리를 행하도록 구성하였지만, 기록 처리 또는 재생 처리가 행해지는 시점에서, 키 갱신 블록(KRB)의 갱신 처리를 행하도록 구성하여도 된다.

다음에, 키 갱신 블록(KRB)의 갱신 처리에 대한 제2 실시예에 대하여 설명한다. 기록 재생 장치 및 기록 매체에서의 키 갱신 블록(KRB)의 갱신 처리에 대하여, 도 19 이후의 도면을 참조하여 설명한다.

도 19A, 도 19B는, 기록 재생 장치에서의 키 갱신 블록(KRB)의 갱신 처리에 대하여 나타낸 것이다. 도 19A는 기록 재생 기기에 기록 매체가 장착되기 이전의 상태로서, 기록 재생 장치(1910)에 하나의 키 갱신 블록(KRB: 1911)이 저장되고, 기록 매체(1920)에는, 2개의 키 갱신 블록(KRB: 1921, 1922)이 저장되어 있 는 상태를 나타내고 있다.

기록 재생 장치(1910)에 저장된 KRB는, 버전(T2)의 키 갱신 블록(KRB: 1911)으로서, 기록 매체(1920)에 저장된 KRB는, 버전(T1)의 키 갱신 블록(KRB: 1921), 및 버전(T3)의 키 갱신 블록(KRB: 1922)이다. 여기 서 버전 T3, T2, T1은, T3이 가장 새롭고, T1이 가장 오래된 것으로 한다.

또한, 기록 매체(1920)에는, 버전(T1)의 키 갱신 블록(KRB)으로부터 생성되는 미디어 키를 이용하여 암호 화된 콘텐츠(1931)가 저장되어 있다.

기록 매체(1920)가 기록 재생 장치(1910)에 장착되고, 기록 재생 장치(1910)에 의해 기록 매체(1920)에 의 액세스가 행해지면, 기록 재생 장치(1910)는 기록 매체(1920) 상의 KRB 중의 최신의 버전의 KRB를 검 색한다. 최신 버전은 T3으로, 버전 T3은 기록 재생 장치(1910)에 저장되어 있는 버전(T2)의 키 갱신 블 록(KRB: 1911)보다도 새롭기 때문에, 그 버전(T3)의 키 갱신 블록(KRB: 1922)을 이용하여 기록 재생 장치 내에 저장하는 KRB를 갱신한다. 그 결과, 도 19B에 도시한 바와 같이, 기록 재생 장치(1910)가 오래된 버전(T2)의 키 갱신 블록(KRB: 1911)은, 새로운 버전의 버전(T3)의 키 갱신 블록(KRB: 1912)으로 치환된 다.

또한, 기록 매체에 저장되어 있는 모든 KRB보다도, 기록 재생 장치가 저장하는 KRB 쪽이 새로운 경우에는, 기록 매체의 액세스 시에 새로운 KRB를 기록 매체에 저장한다. 도 20A, 도 20B는, 기록 재 생 장치가 기록 매체에 새로운 KRB를 기록하는 개념을 나타내고 있다.

도 20A는, 기록 재생 기기에 기록 매체가 장착되기 이전의 상태이고, 기록 재생 장치(2010)에 하나의 키 갱신 블록(KRB: 2011)이 저장되며, 기록 매체(2020)에는 2개의 키 갱신 블록(KRB: 2021, 2022)이 저장되 어 있는 상태를 나타내고 있다.

기록 재생 장치(2010)에 저장된 KRB는, 버전(T3)의 키 갱신 블록(KRB: 2011)으로, 기록 매체(2020)에 저 장된 KRB는, 버전(T1)의 키 갱신 블록(KRB: 2021), 및 버전(T2)의 키 갱신 블록(KRB: 2022)이다. 여기서

버전 T3, T2, T1은, T3이 가장 새롭고, T1이 가장 오래된 것으로 한다.

또한, 기록 매체 (2020)에는, 버전(T1)의 키 갱신 블록(KRB)으로부터 생성되는 미디어 키를 이용하여 암호화된 콘텐츠(2031)가 저장되어 있다.

기록 매체 (2020)가 기록 재생 장치(2010)에 장착되고, 기록 재생 장치(2010)에 의해 기록 매체 (2020)에 액세스가 행해지면, 기록 재생 장치는 기록 매체 (2020) 상의 KRB 중의 최신 버전의 KRB를 검색한다. 최신 버전은 L20이며, 버전 T2는 기록 재생 장치(2010)에 저장되어 있는 버전(T3)의 키 갱신 블록(KRB: 2011)보다도 오래된 버전이기 때문에, 그 버전(T3)의 키 갱신 블록(KRB: 2011)을 기록 매체 (2020)에 기록한다. 그 결과, 도 20B에 도시한 바와 같이, 기록 매체 (2020)에는 새로운 버전의 버전(T3)의 키 갱신 블록(KRB: 2023)이 기록된다.

또한, 본 발명의 기록 재생 장치에서는, 기록 매체에서, 어떤 콘텐츠 데이터의 암호화에도 사용되어 있지 않고, 또한, 기록 매체 상의 최신의 것이 아닌 KRB의 삭제를 실행한다. 도 21A, 도 21B는 기록 재생 장치가 기록 매체 상의 불필요한 KRB를 삭제하는 개념을 나타내고 있다.

도 21A는, 기록 재생 기기에 기록 매체가 장착되기 이전의 상태로서, 기록 재생 장치(2110)에 하나의 키 갱신 블록(KRB: 2111)이 저장되고, 기록 매체 (2120)에는, 3개의 키 갱신 블록(KRB: 2121, 2122, 2123)이 저장되어 있는 상태를 나타내고 있다.

기록 재생 장치(2110)에 저장된 KRB는, 어떠한 임의 버전, 버전(any)의 키 갱신 블록(KRB: 2111)으로서, 기록 매체(2120)에 저장된 KRB는, 버전(T1)의 키 갱신 블록(KRB: 2121), 버전(T2)의 키 갱신 블록(KRB: 2122), 및 버전(T3)의 키 갱신 블록(KRB: 2123)이다. 여기서 버전 T3, T2, T1은, T3이 가장 새롭고, T1이 가장 오래된 것으로 한다.

또한, 기록 매체 (2120)에는, 버전(T1)의 키 갱신 블록(KRB)으로부터 생성되는 미디어 키를 이용하여 암호화된 콘텐츠(2131)가 저장되어 있다.

기록 매체 (2120)가 기록 재생 장치(2110)에 장착되고, 기록 재생 장치(2110)에 의해 기록 매체 (2120)에 액세스가 행해지면, 기록 재생 장치는 어떤 콘텐츠 데이터의 암호화에도 사용되어 있지 않으며, 기록 매체(2120) 상의 최신의 것이 아닌 키 갱신 블록(KRB)을 검색한다. 도 21A, 도 21B의 예에서는, 버전(T2)의 키 갱신 블록(KRB: 2122)이, 그 조건을 만족하는 KRB로서 검출된다. 기록 재생 장치(2110)는, 검출 KRB, 즉, 어떤 콘텐츠 데이터의 암호화에도 사용되어 있지 않으며, 기록 매체(2120) 상의 최신의 것이 아닌 키 갱신 블록(KRB)을 삭제한다. 그 결과, 도 21B에 도시한 바와 같이, 기록 매체(2120)에는, 콘텐츠의 암호화에 사용되고 있는 버전(T1)의 키 갱신 블록(KRB: 2121)과, 가장 새로운 버전의 버전(T3)의 키 갱신 블록(KRB: 2123)만이 기록된 구성으로 된다. 이 결과, 기록 매체의 기록 영역이 유효하게 사용 가능해진다.

이상, 도 19, 도 20, 도 21을 참조하여 설명한 3종류의 KRB 갱신 처리는, 어느 것이나, 예를 들면 기록 재생 장치에 기록 매체가 장착된 시점에서 행하면 된다. 구체적으로는, 도 1의 기록 매체 인터페이스 (190)에 기록 매체가 장착된 것을 검출하면, CPU(170)가, ROM(160), 또는 메모리(170)에 저장된 KRB 갱신 처리 프로그램을 판독하여 실행한다. 이 처리 수순을, 도 22의 흐름도를 참조하여 설명한다.

도 22의 단계 S2201에서는, 기록 재생 장치는 기록 매체 상의 모든 KRB를 검색하고, 그 중에서 최신의 것과, 기록 재생 장치 내의 기록 수단에 저장하고 있는 KRB의 버전(세대)와의 비교 처리를 실행한다. 이들 버전이 동일하면, 아무것도 하지 않고 처리를 종료한다.

기록 매체 상의 최신 KRB가 기록 재생 장치 내의 KRB보다도 새로우면, 단계 S2202로 진행한다. 단계 S2202에서는, 기록 재생 장치가 보유하고 있는 리프 키를 이용하여 갱신 예정의 최신의 KRB가 복호 가능한지의 여부를 판정한다. 즉, 앞의 도 4, 5, 6 등에서 설명한 바와 같이, 자기가 갖는 리프 키, 혹은 노드 키에 의해 키 갱신 블록(KRB)을 순차 복호하고, 세대가 갱신된 세대 정보, (의)신 버전의 노드 키, 예를 들면 K(t)00, 또는 루트 키 K(t)R01 취득 가능한지의 여부를 판정한다. 이 판정 처리는, 예를 들면 도 5에 나타내는 키 갱신 블록(KRB)에서, 어느 하나의 인덱스에 자기가 갖는 리프 키, 노드 키를 그대로 적용하여 복호 가능한 암호화 키가 저장되어 있는지의 여부를 판정함으로써 행해진다.

단계 S2202에서, 기록 재생 장치가 보유하고 있는 리프 키, 노드 키를 이용하여 갱신 예정의 최신의 KRB가 복호 가능이라고 판정된 경우에는, 단계 S2203으로 진행한다. 복호 불가능하고 판정된 경우에는, 단계 S2203을 스킵하여 처리를 종료한다. 단계 S2203에서는, 전술의 도 19를 참조한 설명대로, 기록 매체 상의 최신 KRB를 이용하여 기록 재생 장치 내의 KRB를 갱신하여 처리를 종료한다.

한편, 단계 S2201에서, 기록 재생 장치 내의 KRB가 기록 매체 상의 최신의 KRB보다도 새로운 것이면, 단계 S2204로 진행한다.

단계 S2204에서는, 기록 재생 장치 내의 KRB를 기록 매체에 기록하여, 단계 S2205로 진행한다. 단계 S2205에서는, 기록 매체 상에 불필요한 KRB가 존재하는지를 검사한다. 불필요한 KRB란, 상술한 바와 같이, 기록 매체에 저장된 어떤 콘텐츠 데이터의 암호화에도 사용되어 있지 않고, 또한, 기록 매체 상의 최신의 것이 아닌 KRB의 것이다. 이러한 KRB가 존재한 경우에는, 단계 S2206으로 진행하여, 그 KRB를 기록 매체 상에서 소거하여 처리를 종료한다.

단계 S2205에서, 불필요한 KRB가 존재하지 않은 경우에는, 단계 S2206을 스킵하여 처리를 종료한다. 상기한 바와 같이 하여, 기록 재생 장치 내의 KRB의 갱신, 신규 KRB와 기록 매체에의 기록, 불필요 KRB의 기록 매체로부터의 삭제를 행할 수 있다.

다음에, 도 23의 흐름도를 참조하여, 도 1에 도시한 기록 재생 장치가 기록 매체에 콘텐츠 데이터를 기록하는 처리를 설명한다.

단계 S2301에서, 기록 재생 장치는 자신이 저장하는 KRB로부터 미디어 키를 생성한다. 단계 S2302에서, 이 미디어 키에 기초하여 콘텐츠 데이터를 암호화한다. 구체적인 암호화의 방법으로는, 예를 들면 전

술한 도 7~ 도 11을 참조한 설명에 따른 방법을 이용할 수 있다. 그리고, 암호화한 콘텐츠 데이터를 기록 매체에 기록한다. 이 때, 암호화에 이용한 키를 생성하기 위해 사용한 KRB의 버전(세대)도 기록 매체에 기록한다. KRB의 버전(세대)은 구체적으로는 예를 들면, 도 7에 도시한 타이틀 키(Title Key)나 기록 시대, 번호와 마찬가지로, 어떤 데이터가 어떤 타이틀을 구성하는지 등의 정보가 저장되는 데이터 관리 파일에 기록할 수 있다. 이상의 처리에 의해, 암호화 콘텐츠 데이터 및 그 재생에 필요해지는 KRB 정보를 기록 매체에 기록할 수 있다.

또, 기록 매체에 대한 콘텐츠의 암호화 및 저장 처리에서, 기록 매체에 저장된 키 갱신 블록(KRB), 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록(KRB)중에서 이용 가능한 최신의 키 갱신 블록(KRB)을 검출하여, 검출한 이용 가능한 최신의 키 갱신 블록(KRB)의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 구성으로 함으로써, 보다 새로운 키에 의한 콘텐츠의 암호화, 저장이 촉진된다.

다음에, 상기한 바와 같이 하여 기록된 콘텐츠 데이터를, 기록 매체로부터 기록 재생 장치가 판독하는 처리를, 도 24의 흐름도를 참조하여 설명한다.

단계 S2401에서, 기록 재생 장치는, 재생하는 콘텐츠 데이터를 암호화한 미디어 키를 생성하는 KRB의 버전(세대)을 판독한다. 기록 매체 상의 각 콘텐츠 데이터에 대응하는 KRB의 버전(세대)은, 예를 들면 전술의 데이터 관리 파일에 기록되어 있다.

단계 S2402에서, 기록 재생 장치는 기록 매체 상에 저장되어 있는 KRB 중, 상기한 버전(세대)의 값을 갖는 것을 찾아내고, 이것을 이용하여 전술한 도 6 외의 것을 참조하여 설명한 수순에 따라 미디어 키를 생성한다.

단계 S2403에서, 기록 재생 장치는 기록 매체로부터 콘텐츠 데이터를 판독하고, S2402에서 생성한 미디어 키에 기초하여 이것을 복호하여 사용한다. 이상의 처리에 의해 기록 매체에 저장된 콘텐츠 데이터를 재생할 수 있다.

또, 기록 매체에 저장된 암호 데이터의 복호 처리에서, 기록 매체에 저장된 키 갱신 블록(KRB)뿐만 아니라, 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록(KRB) 중에서, 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록(KRB)을 검출하고, 검출된 키 갱신 블록(KRB)의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여 기록 매체에 저장된 암호데이터의 복호 처리를 실행하는 구성으로 하여도 된다.

이와 같이, 본 발명의 정보 기록 재생 장치에서는, 복수의 다른 세대, 즉 버전을 갖는 키나 갱신 블록(KRB)이 병용되어 있는 환경에서, 복수의 세대, 버전이 다른 키를 기록 매체에 저장 가능하게 하고, 기록 재생 장치가 기록 매체에 액세스했을 때에, 보다 새로운 키를 기록 매체에 저장하고, 또한, 기록 매체로부터 최신의 KRB를 기록 재생 장치 자신의 메모리에 저장하고, 또한, 기록 매체로부터 불필요 키를 삭제하는 구성으로 하였다.

기록 매체에 저장되어 있는 모든 KRB보다도 새로운 KRB를 갖는 기록 재생 장치는, 콘텐츠 데이터를 기록하지 않은 경우에도, 새로운 KRB를 기록 매체에 기록할 수 있게 되어, 이 때문에, 새로운 KRB의 마이그레이션 속도가 빠르게 된다. 이를 처리에 의해, 기록 재생 장치에는 점점 새로운 KRB가 저장되고, 또한 데이터가 기록될 때는, 그 시점에서 기록 재생 장치와 기록 매체가 저장하는 최신의 KRB에 의해 산출되는 미디어 키를 이용하여 데이터가 암호화되어 기록되기 때문에, 예를 들어 기록 매체가 재조된 것이 아무리 오래되고, 사전에 기록 매체에 저장되어 있는 KRB가 오래된 것이었다고 해도, 반대로 기록 재생 장치에 저장되어 있던 KRB가 오래된 것이었다고 해도, 데이터가 기록될 때에는 새로운 KRB가 사용될 가능성이 높아지는 것이 기대되어, 그 데이터의 안전성을 보다 높게 지키는 것이 가능해진다. 따라서, 본 발명의 구성에 따르면, 영화나 음악 등의 저작권이 있는 데이터가 부정한(저작권자의 의사에 반하는) 복제를 효과적으로 방지할 수 있는 기록 시스템을 구성할 수 있다. 또한, 기록 매체 상에 불필요한 KRB, 즉, 콘텐츠 데이터의 암호화에는 사용되어 있지 않고, 또한, 그 기록 매체 상의 KRB 중 최신이 아닌 KRB를 기록 재생 장치가 기록 매체 상에서 소거하는 구성이기 때문에, 기록 매체의 기록 용량을 절약하는 것이 가능해진다.

또, 상술의 실시예의 설명에서는, 미디어 키를 암호 처리용 키로서 이용하는 예를 중심으로하여 설명하였지만, KRB에 의해 갱신되는 암호 처리용 키는, 예를 들면 복수의 정보 기록 장치에 공통인 마스터 키, 정보 기록 재생 장치에 고유의 디바이스 키어도 되고, 상기한 KRB에 의한 키 갱신은, 마스터 키, 디바이스 키에 대해서도, 미디어 키와 마찬가지로 처리가 적용 가능하다.

또한, 상술의 실시예에서는, 기록 매체(1920)가 기록 재생 장치(1910)에 장착된 시점에 기록 매체의 TOC(Table of Contents) 등에 액세스할 때에 키 갱신 블록(KRB)의 갱신 처리를 행하도록 구성하였지만, 기록 처리 혹은 재생 처리가 행해지는 시점에서 기록 매체에 액세스할 때, 키 갱신 블록(KRB)의 갱신 처리를 행하도록 구성하여도 된다.

그런데, 콘텐츠의 저작권자 등의 이익을 보호하기 위해서는 라이선스를 받은장치에서, 콘텐츠의 복사를 제어할 필요가 있다.

즉, 콘텐츠를 기록 매체에 기록하는 경우에는, 그 콘텐츠가, 복사해도 되는(복사 가능)인지의 여부를 조사하여, 복사해도 되는 콘텐츠만을 기록하도록 할 필요가 있다. 또한, 기록 매체에 기록된 콘텐츠를 재생하여 출력하는 경우에는, 그 출력하는 콘텐츠가, 후에, 위법 복사되지 않도록 할 필요가 있다.

그래서, 그와 같은 콘텐츠의 복사 제어를 행하면서, 콘텐츠의 기록 재생을 행하는 경우의 도 1의 기록 재생 장치의 처리에 대하여, 도 25 및 도 26의 흐름도를 참조하여 설명한다.

우선, 외부로부터의 디지털 신호의 콘텐츠를, 기록 매체에 기록하는 경우에는, 도 25A의 흐름도에 따른 기록 처리가 행해진다. 도 25A의 처리에 대하여 설명한다. 여기서는, 도 1의 기록 재생기(100)를 예로 하여 설명한다. 디지털 신호의 콘텐츠(디지털 콘텐츠)가, 예를 들면, IEEE 1394 직렬 버스 등을 통해 입

출력 1/F(120)에 공급되면, 단계 S2501에서, 입력력 1/F(120)는, 그 디지털 콘텐츠를 수신하여, 단계 S2502로 진행한다.

단계 S2502에서는, 입력력 1/F(120)는 수신한 디지털 콘텐츠가, 복사 가능인지의 여부를 판정한다. 즉, 예를 들면, 입력력 1/F(120)가 수신한 콘텐츠가 암호화되어 있지 않은 경우(예를 들면, 상술의 DTCP를 사용하지 않고, 평문의 콘텐츠가, 입력력 1/F(120)에 공급된 경우)에는, 그 콘텐츠는, 복사 가능이라고 판정된다.

또한, 기록 재생 장치(100)가 DTCP에 준거하고 있는 장치로 하고, DTCP에 따라 처리를 실행하도록 한다. DTCP에서는, 복사를 제어하기 위한 복사 제어 정보로서의 2비트의 EMI(Encryption Mode Indicator)가 규정되어 있다. EMI가 008(8)는, 그 이전의 값이 2진수인 것을 나타냄)인 경우에는, 콘텐츠가 무제한 복사(copy-freely)인 것을 나타내며, EMI가 018인 경우에는, 콘텐츠가, 그 이상의 복사를 할 수 없는 것(no-more-copies)인 것을 나타낸다. 또한, EMI가 108인 경우에는, 콘텐츠가, 1번만 복사하여야 하는(Copy-one-generation) 것을 나타내며, EMI가 118인 경우에는, 콘텐츠가 복사가 금지되어 있는 것(Copy-never)인 것을 나타낸다.

기록 재생 장치(100)의 입력력 1/F(120)에 공급되는 신호에 EMI가 포함되고, 그 EMI가, Copy-freely나 Copy-one-generation일 때는 콘텐츠는 복사 가능이라고 판정된다. 또한, EMI가 No-more-copies나 Copy-never일 때는, 콘텐츠는 복사 가능이 아니라고 판정된다.

단계 S2502에서, 콘텐츠가 복사 가능이 아니라고 판정된 경우, 단계 S2503~S2504를 스킵하여, 기록 처리를 종료한다. 따라서, 이 경우에는, 콘텐츠는 기록 매체(10)에 기록되지 않는다.

또한, 단계 S2502에서, 콘텐츠가 복사 가능이라고 판정된 경우, 단계 S2503으로 진행하고, 이하, 단계 S2503~단계 S2504에서, 도 2A의 단계 S202, 단계 S203에서의 처리와 마찬가지로 처리가 행해진다. 즉, 암호 처리 수단(150)에서의 암호화 처리가 실행되고, 그 결과 얻어지는 암호화 콘텐츠를, 기록 매체(195)에 기록하여, 기록 처리를 종료한다.

또, EMI는 입력력 1/F(120)에 공급되는 디지털 신호에 포함되는 것으로, 디지털 콘텐츠가 기록되는 경우에는, 그 디지털 콘텐츠와 함께, EMI, 혹은, EMI와 마찬가지로 복사 제어 상태를 나타내는 정보(예를 들면, DTCP에서의 embedded CCI 등)도 기록된다.

이 때, 일반적으로는, Copy-One-Generation을 나타내는 정보는, 그 이상의 복사를 허용하지 않도록, No-more-copies로 변환되어 기록된다.

외부로부터의 아날로그 신호의 콘텐츠를, 기록 매체에 기록하는 경우에는, 도 25B의 흐름도에 따른 기록 처리가 행해진다. 도 25B의 처리에 대하여 설명한다. 아날로그 신호의 콘텐츠(아날로그 콘텐츠)가, 입력력 1/F(140)에 공급되면, 입력력 1/F(140)는, 단계 S2511에서, 그 아날로그 콘텐츠를 수신하여, 단계 S2512으로 진행하고, 수신한 아날로그 콘텐츠가, 복사 가능인지의 여부를 판정한다.

여기서, 단계 S2512의 판정 처리는, 예를 들면, 입력력 1/F(140)로 수신한 신호에, 매크로비전(Macrovision) 신호나, CGMS-A(Copy Generation Management System-Analog) 신호가 포함되는지 여부에 기초하여 행해진다. 즉, 매크로비전 신호는 VHS 방식의 비디오 카세트 테이프에 기록하면, 노이즈로 된 신호이고, 이것이, 입력력 1/F(140)로 수신한 신호에 포함되는 경우에는, 아날로그 콘텐츠는 복사 가능이 아니라고 판정된다.

또한, 예를 들면, CGMS-A 신호는, 디지털 신호의 복사 제어에 이용되는 CGMS 신호를, 아날로그 신호의 복사 제어에 적용한 신호로, 콘텐츠가 무제한 복사, 1번만 복사, 또는 복사가 금지되어 있는 것 중 어떠한 것인지를 나타낸다.

따라서, CGMS-A 신호가, 입력력 1/F(140)로 수신한 신호에 포함되며, 또한, 그 CGMS-A 신호가, Copy-freely나 Copy-one-generation을 나타내고 있는 경우에는, 아날로그 콘텐츠는, 복사 가능이라고 판정된다. 또한, CGMS-A 신호가, Copy-never를 나타내고 있는 경우에는, 아날로그 콘텐츠는, 복사 가능이 아니라고 판정된다.

또한, 예를 들면, 매크로비전 신호도, CGMS-A 신호도, 입력력 1/F(140)로 수신한 신호에 포함되지 않는 경우에는, 아날로그 콘텐츠는, 복사 가능이라고 판정된다.

단계 S2512에서, 아날로그 콘텐츠가 복사 가능이 아니라고 판정된 경우, 단계 S2513 내지 S2516을 스킵하여, 기록 처리를 종료한다. 따라서, 이 경우에는, 콘텐츠는 기록 매체(195)에 기록되지 않는다.

또한, 단계 S2512에서, 아날로그 콘텐츠가 복사 가능이라고 판정된 경우, 단계 S2513으로 진행하고, 이하, 단계 S2513 내지 S2516에서, 도 2B의 단계 S222 내지 S225에서의 처리와 마찬가지로 처리가 행해지고, 이에 따라, 콘텐츠가 디지털 변환, MPEG 부호화, 암호화 처리가 이루어져 기록 매체에 기록되며, 기록 처리를 종료한다.

또, 입력력 1/F(140)로 수신한 아날로그 신호에, CGMS-A 신호가 포함되어 있는 경우에, 아날로그 콘텐츠를 기록 매체에 기록하기 위해서는, 그 CGMS-A 신호도, 기록 매체에 기록된다. 이 때, 일반적으로는, Copy-One-Generation을 나타내는 정보는, 그 이상의 복사를 허용하지 않도록 No-more-copies로 변환되어 기록된다. 단, 시스템에서 예를 들면 「Copy-one-generation의 복사 제어 정보는, No-more-copies로 변환하지 않고 기록하거나, No-more-copies로서 취급한다」 등의 일이 정해져 있는 경우에는, 이것으로 한정되지는 않는다.

다음에, 기록 매체에 기록된 콘텐츠를 재생하여, 디지털 콘텐츠로서 외부로 출력하는 경우에는, 도 26A의 흐름도에 따른 재생 처리가 행해진다. 도 26A의 처리에 대하여 설명한다. 최초로, 단계 S2601, S2602에서, 도 3A의 단계 S301, S302에서의 처리와 마찬가지로 처리가 행해지고, 이에 따라, 기록 매체로부터 판독된 암호화 콘텐츠가 암호 처리 수단(150)에서 복호 처리가 이루어져, 복호 처리가 실행된 디지털 콘텐츠는 버스(110)를 통해 입력력 1/F(120)에 공급된다.

입출력 I/F(120)는, 단계 S2603에서, 거기에 공급되는 디지털 콘텐츠가, 후에 복사 가능한 것인지의 여부를 판정한다. 즉, 예를 들면, 입출력 I/F(120)에 공급되는 디지털 콘텐츠에 EMI, 혹은, EMI와 마찬가지로 복사 제어 상태를 나타내는 정보(복사 제어 정보)가 포함되지 않는 경우에는, 그 콘텐츠는, 후에 복사 가능한 것이라고 판정된다.

또한, 예를 들면, 입출력 I/F(120)에 공급되는 디지털 콘텐츠에 EMI 등의 복사 제어 정보가 포함되는 경우, 따라서, 콘텐츠의 기록 시에, DTCP의 규격에 따라 EMI가 기록된 경우에는, 그 EMI(기록된 EMI(Recorded EMI))가, Copy-freely일 때는 콘텐츠는, 후에 복사 가능한 것이라고 판정된다. 또한, EMI가, No-more-copies 일 때는 콘텐츠는 후에 복사 가능한 것이 아니라고 판정된다.

또, 일반적으로는, 기록된 EMI가, Copy-one-generation이나 Copy-never인 것은 아니다. Copy-one-generation의 EMI는 기록 시에 No-more-copies로 변환되고, 또한, Copy-never의 EMI를 갖는 디지털 콘텐츠는 기록 매체에 기록되지 않기 때문이다. 단, 시스템에서 예를 들면 「Copy-one-generation의 복사 제어 정보는, No-more-copies로 변환하지 않고 기록하지만, No-more-copies로서 취급한다」 등의 물이 정해져 있는 경우에는, 이것으로 한정되지는 않는다.

단계 S2603에서, 콘텐츠가, 후에 복사 가능한 것이라고 판정된 경우, 단계 S2604로 진행하고, 입출력 I/F(120)는 그 디지털 콘텐츠를, 외부로 출력하고, 재생 처리를 종료한다.

또한, 단계 S2603에서, 콘텐츠가, 후에 복사 가능한 것이 아니라고 판정된 경우, 단계 S2605로 진행하고, 입출력 I/F(120)는, 예를 들면, DTCP의 규격 등에 따라, 디지털 콘텐츠를, 그 디지털 콘텐츠가 후에 복사 되지 않는 형태로 외부로 출력하고, 재생 처리를 종료한다.

즉, 예를 들면, 상술된 바와 같이, 기록된 EMI가, No-more-copies인 경우(혹은, 시스템에서 예를 들면 「Copy-one-generation의 복사 제어 정보는, No-more-copies로 변환하지 않고 기록하지만, No-more-copies로서 취급한다」라는 물이 정해져 있어서, 그 조건 하에서 기록된 EMI가 Copy-one-generation인 경우)에는, 콘텐츠는, 그 이상의 복사는 허용되지 않는다.

이 때문에, 입출력 I/F(120)는, DTCP의 규격에 따른, 상대의 장치 사이에서 인증을 서로 행하여, 상대가 정당한 장치인 경우(여기서는, DTCP의 규격에 준거한 장치인 경우)에는, 디지털 콘텐츠를 암호화하여, 외부로 출력한다.

다음에, 기록 매체에 기록된 콘텐츠를 재생하여, 아날로그 콘텐츠로서 외부로 출력하는 경우에는, 도 268의 흐름도에 따른 재생 처리가 행해진다. 도 268의 처리에 대하여 설명한다. 단계 S2611 내지 단계 S2614에서, 도 38의 단계 S321 내지 단계 S324에서의 처리와 마찬가지로의 처리가 행해진다. 즉, 암호화 콘텐츠의 판독, 복호 처리, MPEG 디코드, D/A 변환이 실행된다. 이에 따라 얻어지는 아날로그 콘텐츠는 입출력 I/F(140)로 수신된다.

입출력 I/F(140)는 단계 S2615에서, 거기에 공급되는 콘텐츠가, 후에 복사 가능한 것인지의 여부를 판정한다. 즉, 기록되어 있던 콘텐츠에 EMI 등의 복사 제어 정보가 함께 기록되어 있지 않은 경우에는, 그 콘텐츠는, 후에 복사 가능한 것이라고 판정된다.

또한, 콘텐츠의 기록 시에, 예를 들면, DTCP의 규격에 따라, EMI 등의 복사 제어 정보가 기록된 경우에는, 그 정보가, Copy-freely일 때는, 콘텐츠는 후에 복사 가능한 것이라고 판정된다.

또한, EMI 등의 복사 제어 정보가, No-more-copies인 경우, 혹은, 시스템에서 예를 들면 「Copy-one-generation의 복사 제어 정보는, No-more-copies로 변환하지 않고 기록하지만, No-more-copies로서 취급한다」라는 물이 정해져 있다. 그 조건 하에서 기록된 EMI 등의 복사 제어 정보가 Copy-one-generation인 경우에는, 콘텐츠는 후에 복사 가능한 것이 아니라고 판정된다.

또한, 예를 들면, 입출력 I/F(140)에 공급되는 콘텐츠에 CGMS-A 신호가 포함되는 경우, 따라서, 콘텐츠의 기록 시에, 그 콘텐츠와 함께 CGMS-A 신호가 기록된 경우에는, 그 CGMS-A 신호가, Copy-freely일 때는, 콘텐츠는 후에 복사 가능한 것이라고 판정된다. 또한, CGMS-A 신호가, Copy-never일 때는, 콘텐츠는, 후에 복사 가능한 것이 아니라고 판정된다.

단계 S2615에서, 콘텐츠가, 후에 복사 가능이라고 판정된 경우, 단계 S2616으로 진행하고, 입출력 I/F(140)는 거기에 공급된 아날로그 신호를, 그대로 외부로 출력하여, 재생 처리를 종료한다.

또한, 단계 S2615에서, 콘텐츠가 후에 복사 가능이 아니라고 판정된 경우, 단계 S2617로 진행하고, 입출력 I/F(140)는 아날로그 콘텐츠를, 그 아날로그 콘텐츠가 후에 복사되지 않는 형태로 외부로 출력하고, 재생 처리를 종료한다.

즉, 예를 들면, 상술된 바와 같이, 기록된 EMI 등의 복사 제어 정보가, No-more-copies인 경우(혹은, 시스템에서 예를 들면 「Copy-one-generation의 복사 제어 정보는, No-more-copies로 변환하지 않고 기록하지만, No-more-copies로서 취급한다」라는 물이 정해져 있어, 그 조건 하에서 기록된 EMI 등의 복사 제어 정보가 Copy-one-generation인 경우)에는, 콘텐츠는, 그 이상의 복사는 허용되지 않는다.

이 때문에, 입출력 I/F(140)는 아날로그 콘텐츠에, 예를 들면, 매크로비전 신호나, Copy-never를 나타내는 CGMS-A 신호를 부가하여, 외부로 출력한다. 또한, 예를 들면, 기록된 CGMS-A 신호가, Copy-never인 경우에도, 콘텐츠는, 그 이상의 복사는 허용되지 않는다. 이 때문에, 입출력 I/F(140)는 CGMS-A 신호를 Copy-never로 변경하고, 아날로그 콘텐츠와 함께 외부로 출력한다.

이상과 같이, 콘텐츠의 복사 제어를 행하면서, 콘텐츠의 기록 재생을 행함으로써, 콘텐츠에 허용된 범위 외의 복사(위법 복사)가 행해지는 것을 방지하는 것이 가능해진다.

또, 상술한 일련의 처리는, 하드웨어에 의해 행하는 것은 물론, 소프트웨어에 의해 행할 수도 있다. 즉, 예를 들면, 암호 처리 수단(150)은 암호화/복호 LSI로서 구성하는 것도 가능하지만, 범용의 컴퓨터나, 칩의 마이크로 컴퓨터에 프로그램을 실행시킴에 따라 행하는 구성으로 하는 것도 가능하다. 일련의 처리

를 소프트웨어에 의해 행하는 경우에는, 그 소프트웨어를 구성하는 프로그램이, 범용의 컴퓨터나 1칩의 마이크로 컴퓨터 등에インストール된다. 도 27은, 상술한 일련의 처리를 실행하는 프로그램이インストール된 컴퓨터의 일 실시 형태의 구성예를 나타내고 있다.

프로그램은, 컴퓨터에 내장되어 있는 기록 매체로서의 하드디스크(2705)나 ROM(2703)에 사전에 기록해 둘 수 있다. 또는, 프로그램은 플로피 디스크, CD-ROM(Compact Disc Read Only Memory), MO(Magneto Optical) 디스크, DVD(Digital Versatile Disc), 자기 디스크, 반도체 메모리 등의 제거 가능한 기록 매체(2710)에, 일시적 혹은 영속적으로 저장(기록)해 두는 것이 가능하다. 이러한 제거할 수 있는 기록 매체(2710)는, 소위 패키지 소프트웨어로서 제공할 수 있다.

또, 프로그램은, 상술한 바와 같은 제거 가능한 기록 매체(2710)로부터 컴퓨터에インストール하는 것 외에, 다운로드 사이트에서, 디지털 위성 방송등의, 인공위성을 통해 컴퓨터에 무선으로 전송하거나, LAN(Local Area Network), 인터넷이라고 하는 네트워크를 통해 컴퓨터에 유선으로 전송하고, 컴퓨터에서는, 그와 같이 하여 전송되어 오는 프로그램을, 통신부(2708)에서 수신하여, 내장하는 하드디스크(2705)에インストール하는 것이 가능하다.

컴퓨터는, CPU(Central Processing Unit: 2702)를 내장하고 있다. CPU(2702)에는 버스(2701)를 통해 입출력 인터페이스(2711)가 접속되어 있으며, CPU(2702)는 입출력 인터페이스(2711)를 통해 사용자에 의해 키보드나 마우스 등으로 구성되는 입력부(2707)가 조작됨으로써 지령 입력되면, 그에 따라서, ROM(2703)에 저장되어 있는 프로그램을 실행한다.

또는, CPU(2702)는 하드디스크(2705)에 저장되어 있는 프로그램, 위성 혹은 네트워크로부터 전송되고, 통신부(2708)에서 수신되어 하드디스크(2705)에インストール된 프로그램, 또는 드라이브(2709)에 장착된 제거할 수 있는 기록 매체(2710)로부터 판독되어 하드디스크(2705)에インストール된 프로그램을, RAM(2704)에 로드하여 실행한다.

이에 따라, CPU(2702)는 상술한 흐름도에 따른 처리, 혹은 상술한 블록도의 구성에 의해 행해지는 처리를 행한다. 그리고, CPU(2702)는 그 처리 결과를, 필요에 따라서, 예를 들면, 입출력 인터페이스(2711)를 통해 LCD(Liquid Crystal Display)나 스피커 등으로 구성되는 출력부(2706)로부터 출력, 혹은, 통신부(2708)로부터 송신, 나아가서는, 하드디스크(2705)에 기록시킨다.

여기서, 본 명세서에서, 컴퓨터에 각종 처리를 행하게 하기 위한 프로그램을 기술하는 처리 단계는, 반드시 흐름도로서 기재된 순서에 따라, 시계열로 처리할 필요는 없고, 병렬적 혹은 개별로 실행되는 처리(예를 들면, 병렬 처리 혹은 오브젝트에 의한 처리)도 포함하는 것이다.

또한, 프로그램은, 하나의 컴퓨터에 의해 처리되는 것이어도 되고, 복수의 컴퓨터에 의해 분산 처리되는 것이어도 무방하다. 또한, 프로그램은, 먼 쪽의 컴퓨터에 전송되어 실행되는 것이어도 된다.

또, 본 실시 형태에서는, 콘텐츠의 암호화/복호를 행하는 블록을, 1칩의 암호화/복호 LSI로 구성하는 예를 중심으로 하여 설명하였지만, 콘텐츠의 암호화/복호를 행하는 블록은, 예를 들면, 도 1에 도시한 CPU(170)가 실행하는 1개의 소프트웨어 모듈로서 실행하는 것도 가능하다.

이상, 특정한 실시예를 참조하면서, 본 발명에 대하여 상세히 설명해 왔다. 그러나, 본 발명의 요지를 일탈하지 않는 범위에서 당업자가 그 실시예의 수정이나 대안을 할 수 있는 것은 자명하다. 즉, 예시라는 형태로 본 발명을 개시한 것이고, 한정적으로 해석되어서는 안된다. 본 발명의 요지를 판단하기 위해서는, 이후에 기재하는 청구의 범위 란을 참조하여야 한다.

산인상이유가능성

본 발명에 따른 정보 기록 재생 장치는, 복수의 다른 세대, 버전을 갖는 키 갠신 블록(KRB)을 기록 매체에 저장 가능하게 함과 함께, 최신의 키 갠신 블록(KRB)을 추출하여, 기록 재생 장치 내의 메모리에 저장하는 것을 가능하게 하였다. 또한, 기록 매체에 대한 콘텐츠 저장 처리에서는, 기록 재생 장치 내의 메모리에 저장된 KRB, 및 기록 매체에 저장된 복수의 KRB 중으로부터, 이용 가능한 최신의 키 갠신 블록(KRB)을 검출하여, 그 최신 KRB로부터 암호 처리용의 키, 예를 들면 미디어 키를 취득하여, 취득한 최신의 미디어 키를 이용하여 콘텐츠의 암호화 처리를 실행하여, 기록 매체에 저장하고, 콘텐츠의 암호화에 이용한 예를 들면 미디어 키를 취득한 키 갠신 블록(KRB)을 새롭게 기록 매체에 저장하는 구성으로 하였다. 따라서, 콘텐츠를 기록 매체에 새롭게 기록할 때에는, 보다 새로운 KRB에 기초하여 산출되는 미디어 키를 이용한 암호화가 이루어진다.

따라서, 예를 들면 기록 매체의 제조 시에 콘텐츠 암호화에 이용된 오래된 버전의 KRB가 기록 매체에 저장되었다고 하여도, 보다 새로운 KRB에 기초한 암호 처리 키에 의한 콘텐츠 암호화 및 저장도 가능해진다. 따라서, 키 갠신 처리에 의해 새로운 버전의 KRB를 부정합 기기를 리보크하여 발행함으로써, 그 후에는, 정당한 기기만이 취득 가능한 새로운 버전의 KRB로부터 취득되는 키에 기초한 암호화 콘텐츠를 기록 매체에 저장하는 것이 가능해지므로, 기록 매체 자체의 세대에 상관없이, 신규 저장되는 암호화 콘텐츠에 관해서는, 리보크된 기기에서의 이용 배제가 가능해진다.

또한, 본 발명에 따른 정보 기록 재생 장치는, 기록 재생 장치에는 점점 새로운 KRB가 저장되게 되고, 또한 데이터가 기록될 때에는, 그 시점에서 기록 재생 장치와 기록 매체가 저장하는 최신의 KRB에 의해 산출되는 미디어 키를 이용하여 데이터가 암호화되어 기록되기 때문에, 예를 들어 기록 매체가 제조된 것이 아무리 오래되고, 사전에 기록 매체에 저장되어 있는 KRB가 오래된 것이었다고 해도, 데이터가 기록될 때에는 새로운 KRB가 사용되며, 암호화 콘텐츠는 보다 새로운 버전의 암호 처리 키로 암호화되게 된다. 이 때문에, 본 발명에 따르면, 영화나 음악 등의 저작권이 있는 데이터가 부정합 복제, 예를 들면 저작권자의 뜻에 반하는 복제가 만연되는 것을 방지할 수 있다.

이상, 설명한 바와 같이, 본 발명의 정보 기록 재생 장치는 복수의 세대, 버전이 다른 키를 기록 매체에 저장 가능하게 하고, 기록 재생 장치가 기록 매체에 액세스했을 때, 보다 새로운 키를 기록 매체에 저장

하며, 또한, 기록 매체로부터 최신의 KRB를 기록 재생 장치 자신의 메모리에 저장하고, 또한, 기록 매체로부터 불필요 키를 삭제하는 구성으로 하며, 기록 매체에 저장되어 있는 모든 KRB보다도 새로운 KRB를 갖는 기록 재생 장치는, 콘텐츠 데이터를 기록하지 않는 경우에도, 새로운 KRB를 기록 매체에 기록할 수 있는 구성으로 하였다.

이 때문에, 새로운 KRB의 마이그레이션의 속도가 빠르게 되어, KRB 갱신 처리에 의해 기록 재생 장치에는 점점 새로운 KRB가 저장되고, 또한 데이터가 기록될 때에는, 그 시점에서 기록 재생 장치와 기록 매체가 저장하는 최신의 KRB에 의해 산출되는 미디어 키를 이용하여 데이터가 암호화되어 기록된다. 따라서, 예를 들어 기록 매체가 제조된 것이 아무리 오래되고, 사전에 기록 매체에 저장되어 있는 KRB가 오래된 것이었다고 해도, 또한, 반대로 기록 재생 장치에 저장되어 있던 KRB가 오래된 것이었다고 해도, 데이터가 기록될 때에는 새로운 KRB가 사용되는 가능성이 높게 되어, 암호화 데이터의 안전성을 보다 높게 하는 것이 가능해진다.

따라서, 본 발명의 구성에 의하면, 영화나 음악 등의 저작권이 있는 데이터가 부정한 (저작권자의 의사에 반한) 복제를 효과적으로 방지 가능한 기록 시스템을 구성할 수 있다. 또한, 기록 매체 상의 불필요한 KRB, 즉, 콘텐츠 데이터의 암호화에는 사용되어 있지 않고, 또한, 그 기록 매체 상의 KRB 중 최신이 아닌 KRB를 기록 재생 장치가 기록 매체 상에서 소거하는 구성이므로 기록 매체의 기록 용량을 절약하는 것이 가능해진다.

(5) 청구의 범위

청구항 1

기록 매체에 정보를 기록하는 정보 기록 장치에 있어서,

상기 장치는,

복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과,

상기 정보 기록 장치에 내장한 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하며, 상기 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하고, 그 산출된 암호 처리용 키를 사용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 암호 처리 수단을

을 포함하며,

상기 암호 처리 수단은, 상기 기록 매체에 대한 콘텐츠의 암호화 및 저장 처리에 있어서, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신의 키 갱신 블록을 검출하며, 검출된 이용 가능한 최신의 키 갱신 블록의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여, 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 2

제1항에 있어서,

상기 암호 처리용 키는, 복수의 정보 기록 장치에 공통인 마스터 키, 정보 기록 장치에 고유의 디바이스 키, 기록 매체에 고유하게 설정되는 미디어 키 중 어느 하나인 것을 특징으로 하는 정보 기록 장치.

청구항 3

제1항에 있어서,

상기 정보 기록 장치는, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신이 갖는 키 갱신 블록 중의 이용 가능한 최신의 키 갱신 블록이, 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 기록 매체에 미저장인 경우에 있어서, 기록 매체에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 구성을 더 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 4

제1항에 있어서,

상기 정보 기록 장치는, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신이 갖는 키 갱신 블록 중의 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 기록 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 기록 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 5

제1항에 있어서,

상기 노드 키는 갱신 가능한 키로서 구성되고, 상기 암호 처리용 키 갱신 처리에 있어서, 갱신 노드 키를 하위 계층의 노드 키 또는 리프 키 중 적어도 어느 하나를 포함하는 키에 의해 암호화한 키 갱신 블록을 암호 처리용 키 제공 대상 리프의 정보 기록 장치에 배포하는 구성이며,

상기 정보 기록 장치에서의 상기 암호 처리 수단은,

상기 갱신 노드 키로 암호화 처리한 암호 처리용 키를 수령하고,

키 갱신 블록의 암호 처리에 의해, 상기 갱신 노드 키를 취득함과 함께, 그 취득한 갱신 노드 키에 기초하여 상기 암호 처리용 키를 산출하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 6

제1항에 있어서,

상기 암호 처리용 키는, 세대 정보로서의 버전 번호가 대응된 구성인 것을 특징으로 하는 정보 기록 장치.

청구항 7

기록 매체로부터 정보를 재생하는 정보 재생 장치에 있어서,

상기 장치는,

복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과,

상기 정보 재생 장치에 내장한 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하고, 상기 기록 매체에 저장된 암호 데이터의 복호 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하여, 그 산출된 암호 처리용 키를 사용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 암호 처리 수단

를 포함하며,

상기 암호 처리 수단은,

상기 기록 매체에 저장된 암호 데이터의 복호 처리에 있어서, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중에서, 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하여, 검출한 키 갱신 블록의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 8

제7항에 있어서,

상기 암호 처리용 키는, 복수의 정보 재생 장치에 공통인 마스터 키, 정보 재생 장치에 고유의 디바이스 키, 기록 매체에 고유하게 설정되는 미디어 키 중 어느 하나인 것을 특징으로 하는 정보 재생 장치.

청구항 9

제7항에 있어서,

상기 정보 재생 장치는, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신이 갖는 키 갱신 블록 중의 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 재생 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 재생 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 10

제7항에 있어서,

상기 노드 키는 갱신 가능한 키로서 구성되며, 상기 암호 처리용 갱신 처리에 있어서, 갱신 노드 키를 하위 계층의 노드 키 또는 리프 키 중 적어도 어느 하나를 포함하는 키에 의해 암호화한 키 갱신 블록을 암호 처리용 키 제공 대상 리프의 정보 재생 장치에 배포하는 구성이며,

상기 정보 재생 장치에서의 상기 암호 처리 수단은,

상기 갱신 노드 키로 암호화 처리한 암호 처리용 키를 수령하고,

키 갱신 블록의 암호 처리에 의해, 상기 갱신 노드 키를 취득함과 함께, 취득한 갱신 노드 키에 기초하여 상기 암호 처리용 키를 산출하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 11

제7항에 있어서,

상기 암호 처리용 키는, 세대 정보로서의 버전 번호가 대응된 구성인 것을 특징으로 하는 정보 재생 장치.

청구항 12

복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하여, 기록 매체에 대한 정보 기록을 행하는 정보 기록 장치에서의 정보 기록 방법에 있어서,

기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터

이용 가능한 최신의 키 갱신 블록을 검출하는 검출 단계와,

상기 검출 단계에서, 검출된 이용 가능한 최신의 키 갱신 블록에 대하여, 상기 정보 기록 장치에 내장한 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 키 갱신 블록의 복호 처리를 실행하여, 상기 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하는 복호 처리 단계와,

상기 복호 처리 단계에서, 산출된 암호 처리용 키를 이용하여 상기 기록 매체에 대한 기록 데이터의 암호화를 행하여 기록 매체에 저장하는 단계

를 포함하는 것을 특징으로 하는 정보 기록 방법.

청구항 13

제12항에 있어서,

상기 검출 단계는, 검출한 이용 가능한 최신의 키 갱신 블록이, 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 기록 매체에 미저장인 경우에 있어서, 기록 매체에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 것을 특징으로 하는 정보 기록 방법.

청구항 14

제12항에 있어서,

상기 검출 단계에서, 검출한 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 기록 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 기록 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 것을 특징으로 하는 정보 기록 방법.

청구항 15

복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 보유하고, 기록 매체에 저장된 암호 데이터의 복호 처리를 행하는 정보 재생 장치에서의 정보 재생 방법에 있어서,

기록 매체에 저장되어, 재생 대상이 되는 콘텐츠의 암호 처리용 키의 버전 정보를 취득하는 단계와,

기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터, 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하는 검출 단계와,

상기 검출 단계에서 검출한 키 갱신 블록의 복호 처리에 의해 암호 처리용 키를 생성하는 단계와,

생성한 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 단계를 포함하는 것을 특징으로 하는 정보 재생 방법.

청구항 16

제15항에 있어서,

상기 정보 재생 방법에 있어서,

상기 검출 단계는, 검출한 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 재생 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 재생 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 것을 특징으로 하는 정보 재생 방법.

청구항 17

정보를 기록 가능한 정보 기록 매체에 있어서,

복수의 다른 정보 기록 장치 또는 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 또는 재생 장치 고유의 리프 키에 포함되는 갱신 노드 키를 하위 계층의 노드 키 또는 리프 키 중 적어도 어느 하나를 포함하는 키에 의해 암호화한 키 갱신 블록을, 다른 구성을 갖는 복수의 키 갱신 블록으로서, 저장한 것을 특징으로 하는 정보 기록 매체.

청구항 18

제17항에 있어서,

상기 복수의 키 갱신 블록의 각각은, 세대 정보로서의 버전 번호가 대응된 구성인 것을 특징으로 하는 정보 기록 매체.

청구항 19

복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하고, 기록 매체에 대한 정보 기록을 행하는 정보 기록 장치에서의 정보 기록 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램에 있어서,

기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신의 키 갱신 블록을 검출하는 검출 단계와,

상기 검출 단계에서 검출된 이용 가능한 최신의 키 갱신 블록에 대하여, 상기 정보 기록 장치에 내장한

노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 키 갱신 블록의 복호 처리를 실행하여, 상기 기록 매체에 저장하는 데이터의 암호화 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하는 복호 처리 단계와,

상기 복호 처리 단계에서 산출된 암호 처리용 키를 이용하여 상기 기록 매체에 대한 기록 데이터의 암호화를 행하여 기록 매체에 저장하는 단계

를 포함하는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 20

복수의 다른 정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 보유하고, 기록 매체에 저장된 암호 데이터의 복호 처리를 행하는 정보 재생 장치에서의 정보 재생 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램에 있어서, 기록 매체에 저장되고, 재생 대상이 되는 콘텐츠의 암호 처리용 키의 버전 정보를 취득하는 단계와,

기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터, 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하는 검출 단계와,

상기 검출 단계에서 검출된 키 갱신 블록의 복호 처리에 의해 암호 처리용 키를 생성하는 단계와,

생성한 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 21

기록 매체에 정보를 기록하는 정보 기록 장치에 있어서,

상기 장치는,

복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과,

상기 정보 기록 장치에 저장한 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하여, 상기 기록 매체에 저장하는 데이터의 암호화 처리에 이용한다 암호 처리용 키의 산출 처리를 실행하고, 상기 산출한 암호 처리용 키를 사용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 암호 처리 수단과,

기록 매체에 대한 액세스 시에, 기록 매체에 저장된 키 갱신 블록과, 정보 기록 장치 자신이 갖는 키 갱신 블록과의 버전 비교를 실행하여, 신 버전의 키 갱신 블록이 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록이고, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에 있어서, 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 수단

를 포함하는 것을 특징으로 하는 정보 기록 장치.

청구항 22

제2항에 있어서,

상기 갱신 처리 수단은, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신이 갖는 키 갱신 블록 중의 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 기록 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 기록 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 23

제2항에 있어서,

상기 갱신 처리 수단은, 기록 매체에 저장된 키 갱신 블록 중에, 그 기록 매체에 저장된 어떤 콘텐츠 데이터의 암호화에도 불사용이면서, 그 기록 매체 상의 최신의 것이 아닌 키 갱신 블록의 검출 처리를 실행하고, 검출된 키 갱신 블록을 이 기록 매체 상에서 삭제하는 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 24

제2항에 있어서,

상기 암호 처리 수단은, 상기 기록 매체에 대한 콘텐츠의 암호화 및 저장 처리에 있어서, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신의 키 갱신 블록을 검출하여, 검출한 이용 가능한 최신의 키 갱신 블록의 복호 처리에 의해서 얻어지는 암호 처리용 키를 이용하여 기록 매체에 대한 저장 데이터의 암호화 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 25

제2항에 있어서,

상기 암호 처리용 키는, 복수의 정보 기록 장치에 공통인 마스터 키, 정보 기록 장치에 고유의 디바이스 키, 기록 매체에 고유하게 설정되는 미디어 키 중 어느 하나인 것을 특징으로 하는 정보 기록 장치.

청구항 26

제28항에 있어서,

상기 노드 키는 갱신 가능한 키로서 구성되며, 상기 암호 처리용 키 갱신 처리에 있어서, 갱신 노드 키를 하위 계층의 노드 키 또는 리프 키 중 적어도 어느 하나를 포함하는 키에 의해 암호화한 키 갱신 블록을 암호 처리용 키 제공 대상 리프의 정보 기록 장치에 배포하는 구성이며,

상기 정보 기록 장치에서의 상기 암호 처리 수단은,

상기 갱신 노드 키를 암호화 처리한 암호 처리용 키를 수령하고

키 갱신 블록의 암호 처리에 의해 상기 갱신 노드 키를 취득함과 함께, 그 취득한 갱신 노드 키에 기초하여 상기 암호 처리용 키를 산출하는 구성을 갖는 것을 특징으로 하는 정보 기록 장치.

청구항 27

제28항에 있어서,

상기 암호 처리용 키는, 세대 정보로서의 버전 번호가 대응된 구성인 것을 특징으로 하는 정보 기록 장치.

청구항 28

기록 매체로부터 정보를 재생하는 정보 재생 장치에 있어서,

정보 재생 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 재생 장치 고유의 리프 키를 저장하고, 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 갱신 키 저장 데이터로서 구성되는 키 갱신 블록을 저장하는 메모리 수단과,

상기 정보 재생 장치에 내장한 상기 노드 키 또는 리프 키 중 적어도 어느 하나를 이용하여 복호 가능한 키 갱신 블록의 복호 처리를 실행하여, 상기 기록 매체에 저장된 암호 데이터의 복호 처리에 이용하는 암호 처리용 키의 산출 처리를 실행하고, 그 산출된 암호 처리용 키를 사용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 암호 처리 수단과,

기록 매체에 대한 액세스 시에, 기록 매체에 저장된 키 갱신 블록과, 정보 재생 장치 자신이 갖는 키 갱신 블록과의 버전 비교를 실행하여, 신 버전의 키 갱신 블록이, 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록이며, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에 있어서, 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 수단

을 포함하는 것을 특징으로 하는 정보 재생 장치.

청구항 29

제28항에 있어서,

상기 갱신 처리 수단은, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신이 갖는 키 갱신 블록 중의 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 재생 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 재생 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 30

제28항에 있어서,

상기 갱신 처리 수단은, 기록 매체에 저장된 키 갱신 블록 중에, 그 기록 매체에 저장된 어떤 콘텐츠 데이터의 암호화에도 불사용이면서, 그 기록 매체 상의 최신의 것이 아닌 키 갱신 블록의 검출 처리를 실행하고, 검출된 키 갱신 블록을 이 기록 매체 상에서 삭제하는 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 31

제28항에 있어서,

상기 암호 처리 수단은, 상기 기록 매체에 저장된 암호 데이터의 복호 처리에 있어서, 기록 매체에 저장된 키 갱신 블록, 및 정보 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터, 재생 대상 콘텐츠의 암호 처리용 키의 버전과 일치하는 키 갱신 블록을 검출하여, 검출된 키 갱신 블록의 복호 처리에 의해 얻어지는 암호 처리용 키를 이용하여 기록 매체에 저장된 암호 데이터의 복호 처리를 실행하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 32

제28항에 있어서,

상기 암호 처리용 키는, 복수의 정보 재생 장치에 공통인 마스터 키, 정보 재생 장치에 고유의 디바이스 키, 기록 매체에 고유하게 설정되는 미디어 키 중 어느 하나인 것을 특징으로 하는 정보 재생 장치.

청구항 33

제28항에 있어서,

상기 노드 키는 갱신 가능한 키로서 구성되고, 상기 암호 처리용 키 갱신 처리에 있어서, 갱신 노드 키를

하위계층의 노드 키 또는 리프 키 중 적어도 어느 하나를 포함하는 키에 의해 암호화된 키 갱신 블록을 암호 처리용 키 제공 대장 리프의 정보 재생 장치에 배포하는 구성이며,

상기 정보 재생 장치에서의 상기 암호 처리 수단은,

상기 갱신 노드 키로 암호화 처리한 암호 처리용 키를 수령하고,

키 갱신 블록의 암호 처리에 의해, 상기 갱신 노드 키를 취득함과 함께, 그 취득한 갱신 노드 키에 기초하여 상기 암호 처리용 키를 산출하는 구성을 갖는 것을 특징으로 하는 정보 재생 장치.

청구항 34

제28항에 있어서,

상기 암호 처리용 키는, 세대 정보로서의 버전 번호가 대응된 구성인 것을 특징으로 하는 정보 재생 장치.

청구항 35

복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하여, 기록 매체에 대한 정보 기록을 행하는 정보 기록 또는 재생 장치에서의 암호 처리 키 갱신 방법에 있어서,

기록 매체에 저장된 키 갱신 블록, 및 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신 버전의 키 갱신 블록을 검출하는 검출 단계와,

최신 버전의 키 갱신 블록이 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록이고, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에 있어서, 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 단계

를 포함하는 것을 특징으로 하는 암호 처리 키 갱신 방법.

청구항 36

제35항에 있어서,

상기 갱신 처리 단계는, 또한, 기록 매체에 저장된 키 갱신 블록, 및 정보 기록 또는 재생 장치 자신이 갖는 키 갱신 블록 중의 이용 가능한 최신의 키 갱신 블록이, 기록 매체에 저장한 키 갱신 블록이며, 그 최신의 키 갱신 블록이 정보 기록 또는 재생 장치 자신의 메모리에 미저장인 경우에 있어서, 정보 기록 또는 재생 장치 자신의 메모리에 대한 상기 최신의 키 갱신 블록의 기입 처리를 실행하는 단계를 포함하는 것을 특징으로 하는 암호 처리 키 갱신 방법.

청구항 37

제36항에 있어서,

상기 갱신 처리 단계는, 기록 매체에 저장된 키 갱신 블록 중에, 그 기록 매체에 저장된 어떤 콘텐츠 데이터의 암호화에도 사용되지 않으면서, 그 기록 매체 상의 최신의 것이 아닌 키 갱신 블록의 검출 처리를 실행하고, 검출된 키 갱신 블록을 이 기록 매체 상에서 삭제하는 처리를 실행하는 단계를 더 포함하는 것을 특징으로 하는 암호 처리 키 갱신 방법.

청구항 38

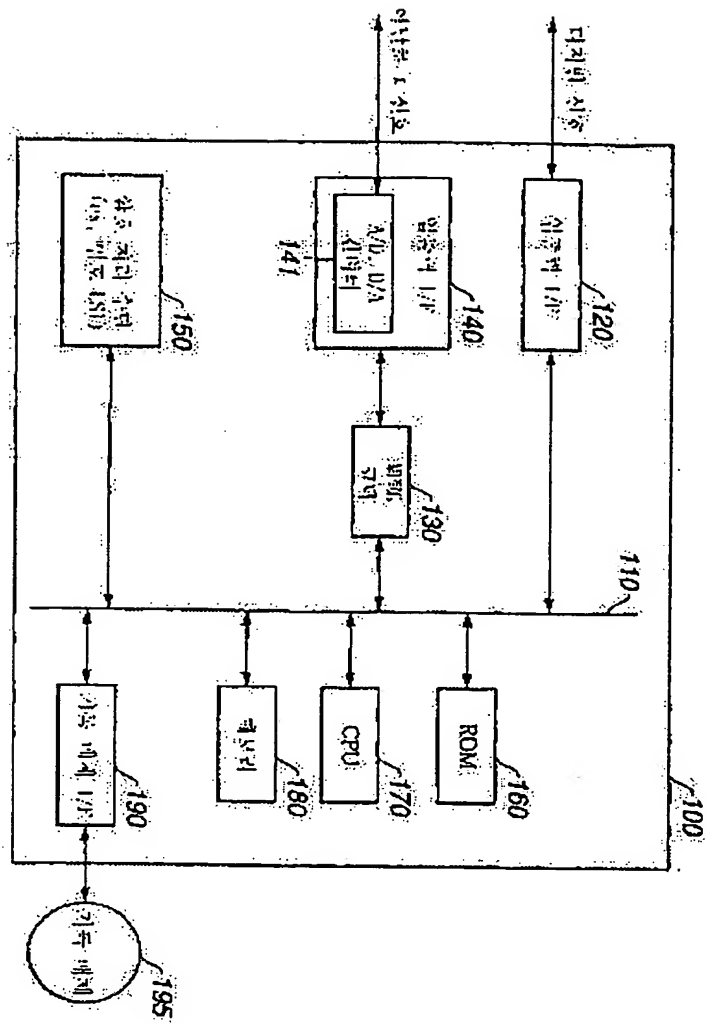
복수의 다른 정보 기록 장치를 리프로 한 계층 트리 구조를 구성하는 각 노드에 고유의 노드 키와 각 정보 기록 장치 고유의 리프 키를 보유하고, 기록 매체에 대한 정보 기록 재생을 행하는 정보 기록 또는 재생 장치에서의 암호 처리 키 갱신 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램에 있어서,

기록 매체에 저장된 키 갱신 블록, 및 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록 중으로부터 이용 가능한 최신 버전의 키 갱신 블록을 검출하는 검출 단계와,

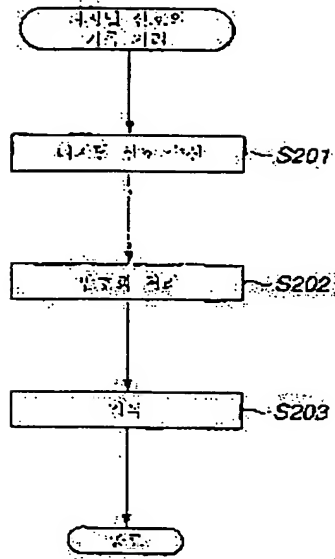
최신 버전의 키 갱신 블록이 정보 기록 또는 재생 장치 자신의 메모리에 저장한 키 갱신 블록이며, 그 신 버전의 키 갱신 블록이 기록 매체에 미저장인 경우에 있어서, 기록 매체에 대한 상기 신 버전의 키 갱신 블록의 기입 처리를 실행하는 갱신 처리 단계

를 포함하는 것을 특징으로 하는 컴퓨터 프로그램.

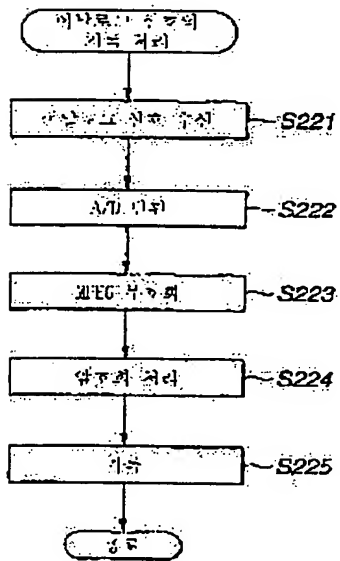
도면



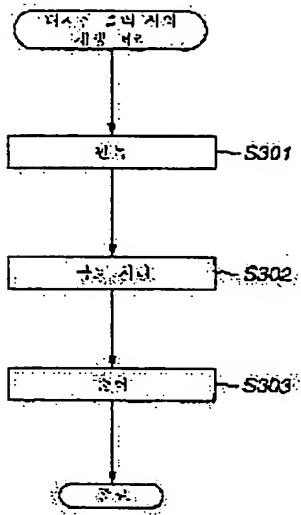
도면28



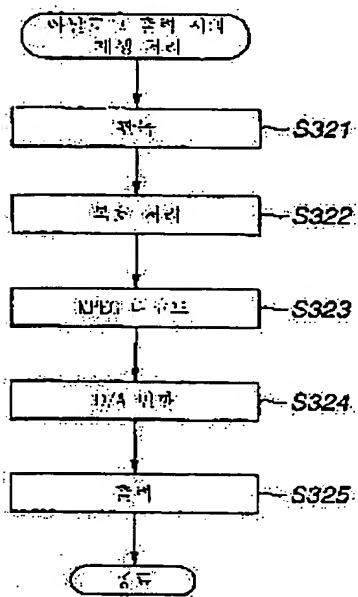
도면29



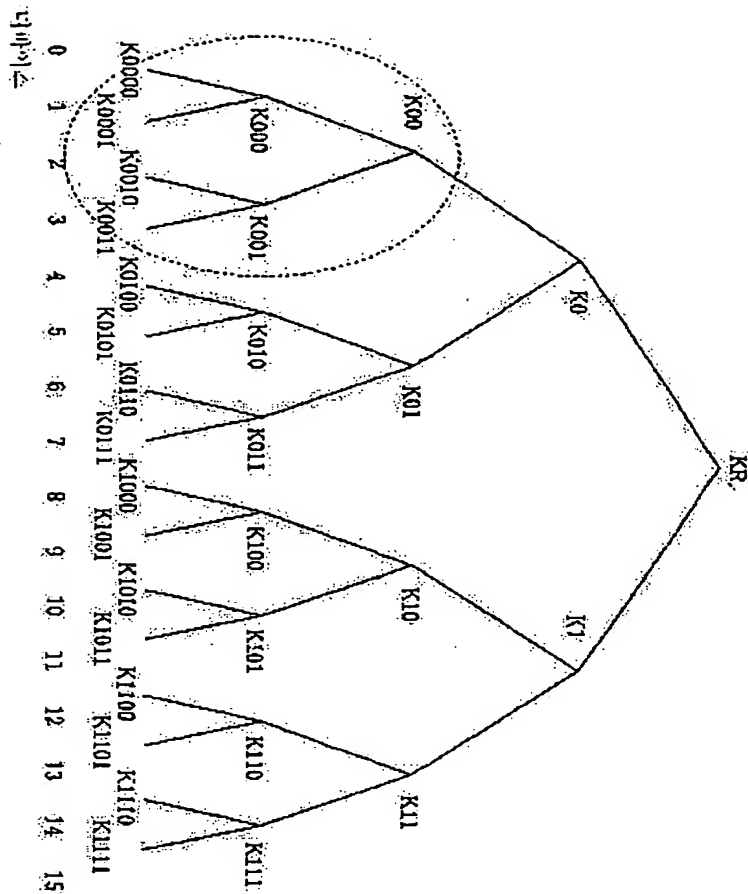
도면31



도면32



도면4



도면5

제 1 생성 블록 (KRB : Key Renewal Block) 에 1
비트인 0, 1, 2에 1 치환이시여 두드 기 K(t)를 상부

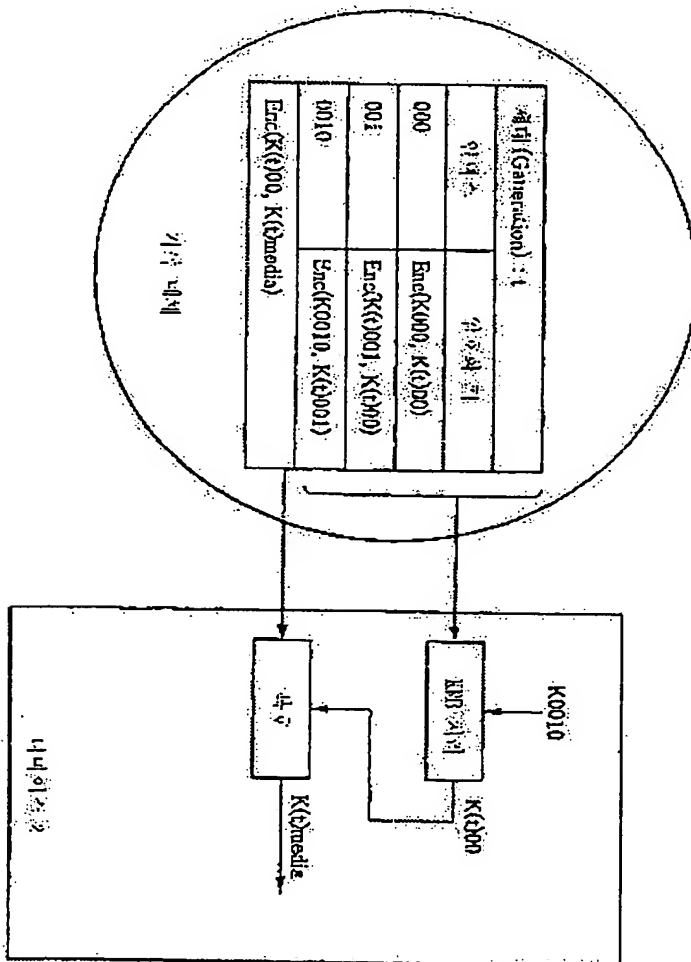
세대 (Generation) : t	
위치	값
0	$Enc(K(t)0, K(t)R)$
00	$Enc(K(t)00, K(t)0)$
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

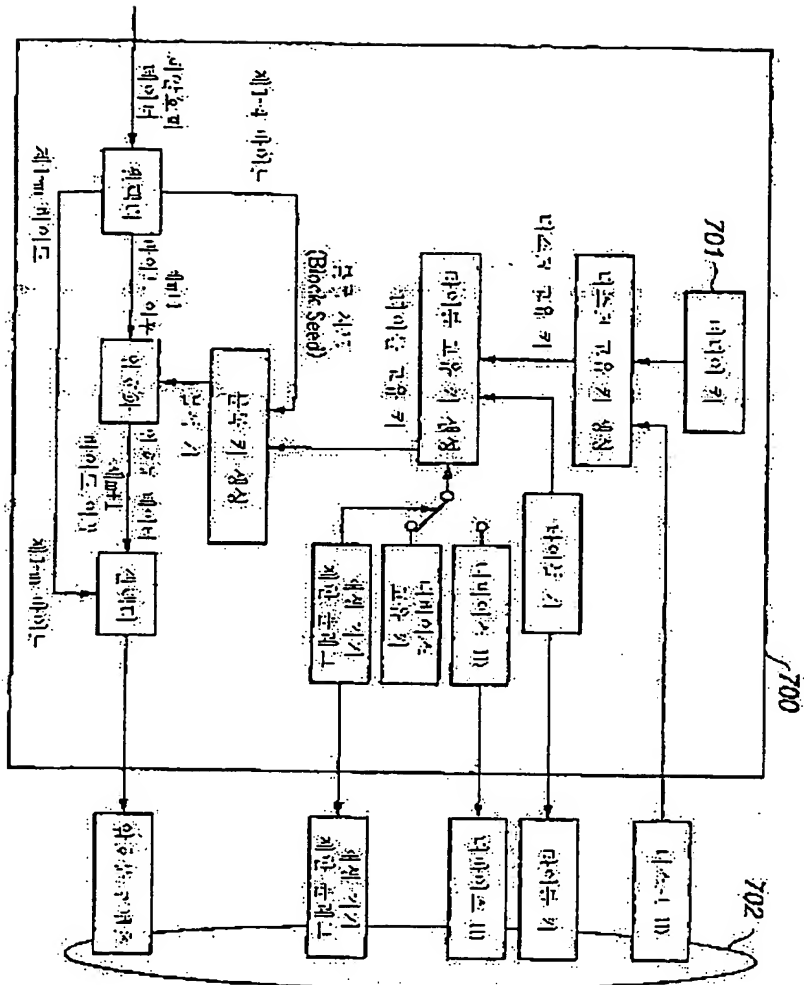
도 158

키 갱신 블록 (KRB : Key Renewal Block)의 2
비트인 0, 1, 2에 1 시퀀스 번호의 1, 1, 1 키 K(1)R을 송신

세대 (Generation) : 1	
인덱스	암호화 키
000	Enc(K000, K(1)00)
001	Enc(K(1)001, K(1)00)
0010	Enc(K0010, K(1)001)

도 159



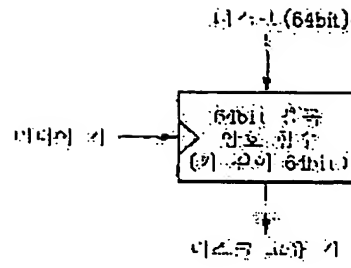


도면 8

예 1

디스크 공유 키 생성에

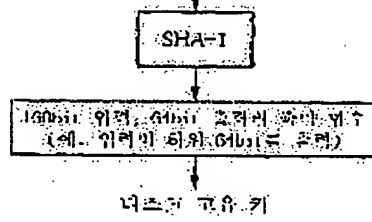
입력
미디어 키 (64bit)
디스크 ID (64bit)



출력
디스크 공유 키 (64bit)

예 2

미디어 키 || 디스크 ID



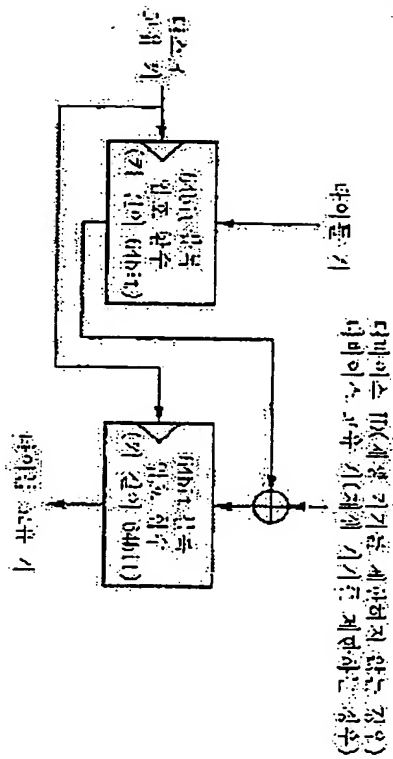
나이를 먹고 싶어서

다이어트 키(64bit)

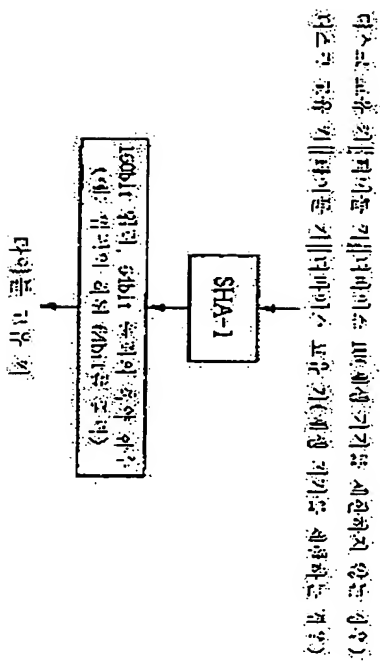
다스고 (Mabit) 또는
다비아스 (Mabit)

다미트 가브(64bit)

3



ॐ

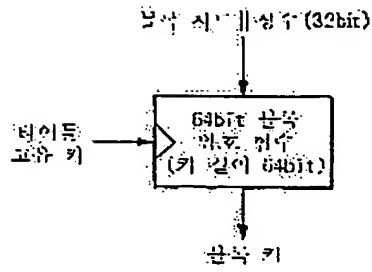


도면 10

예 1

문득 키 생성기

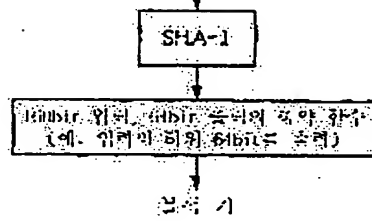
입력
문득 키(32bit)
다익슨 곱셈 키(64bit)



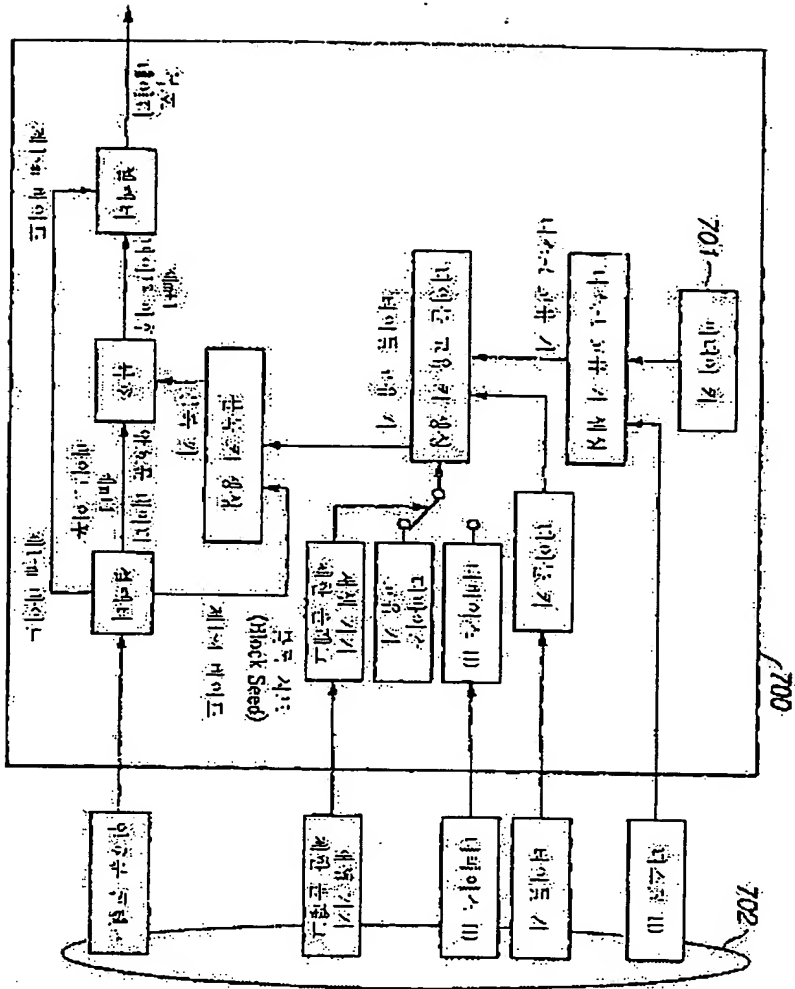
출력
문득 키(64bit)

예 2

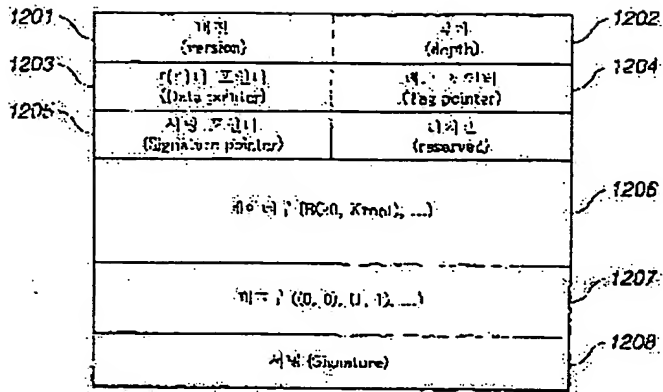
다익슨 곱셈 키 || 문득 키



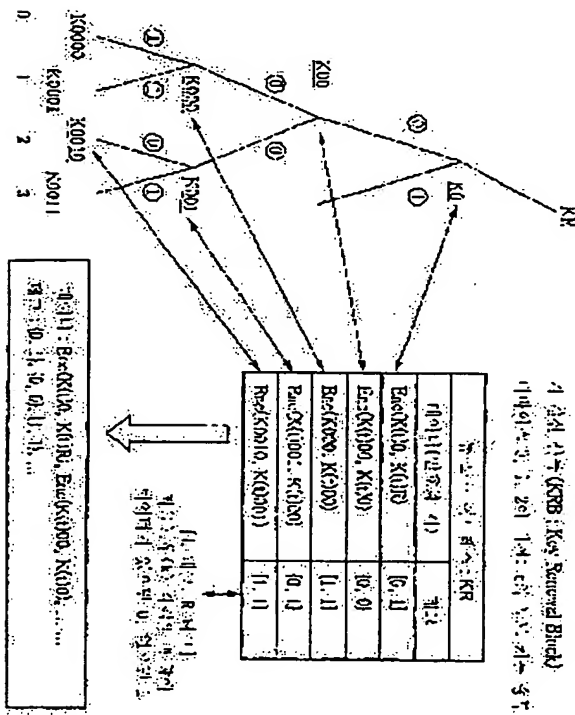
도면 11



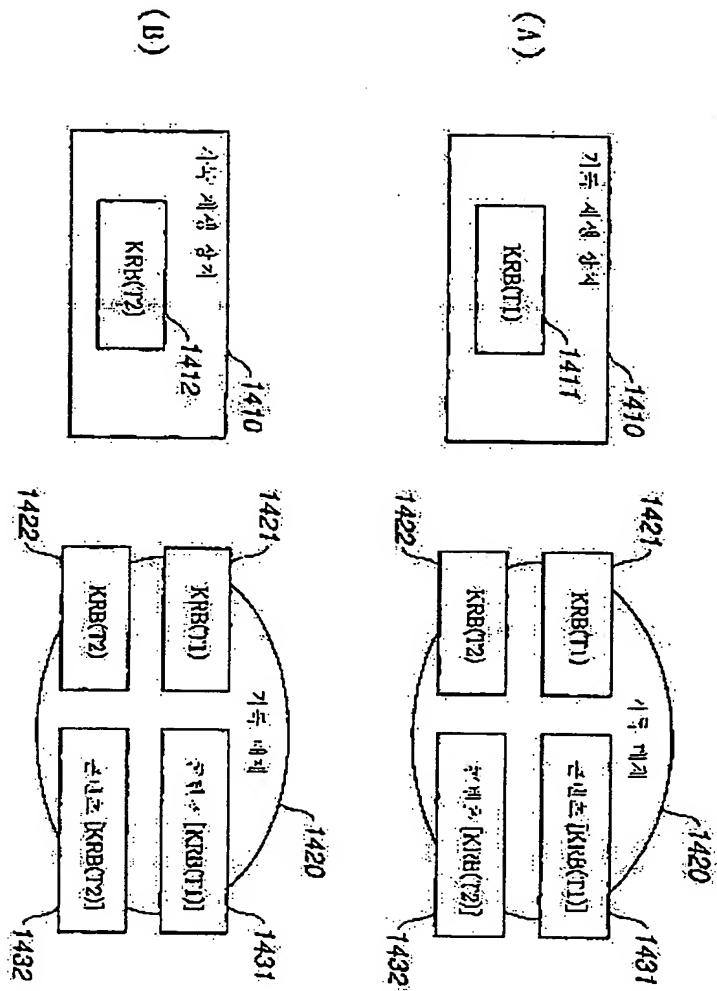
도 12



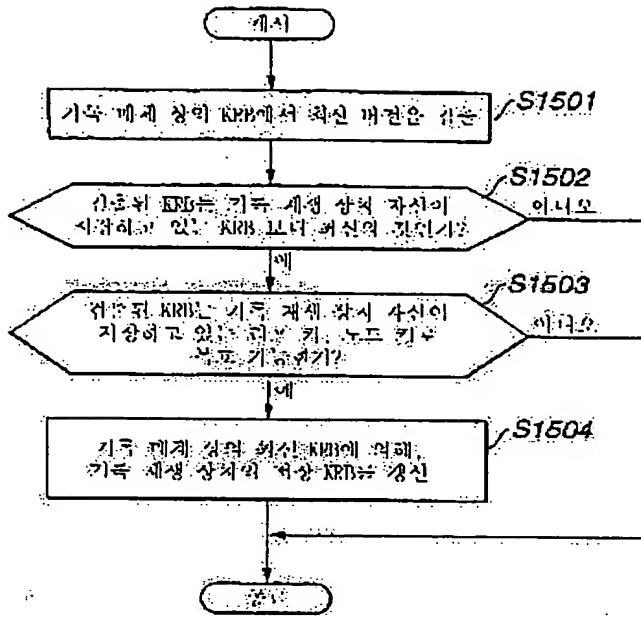
도 13



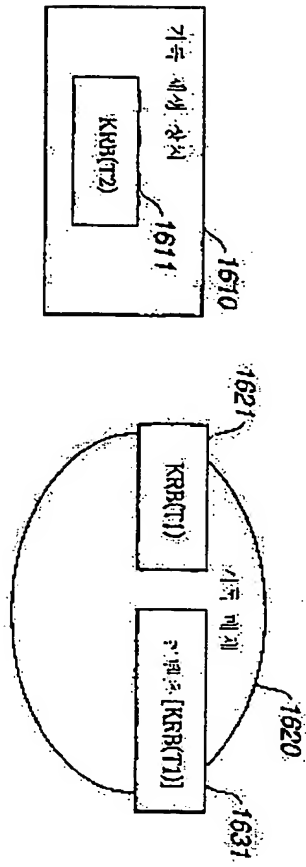
도면 14



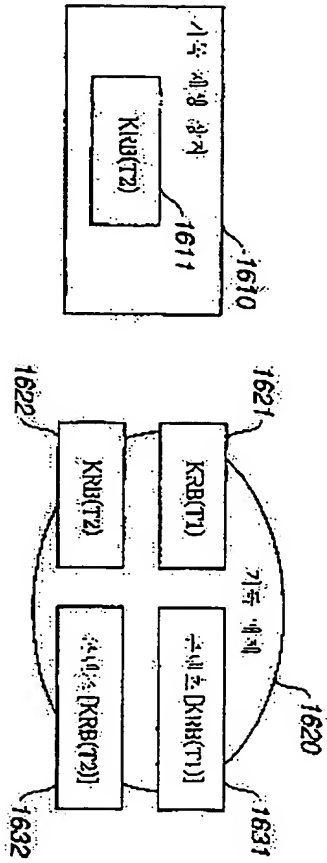
도면 15



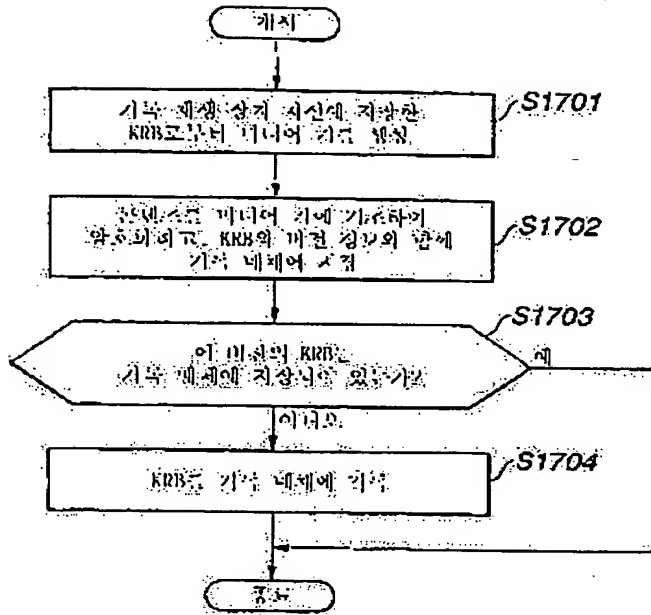
도면 181



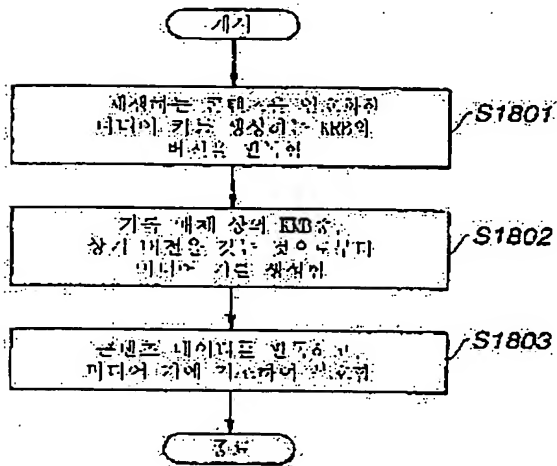
도면 160



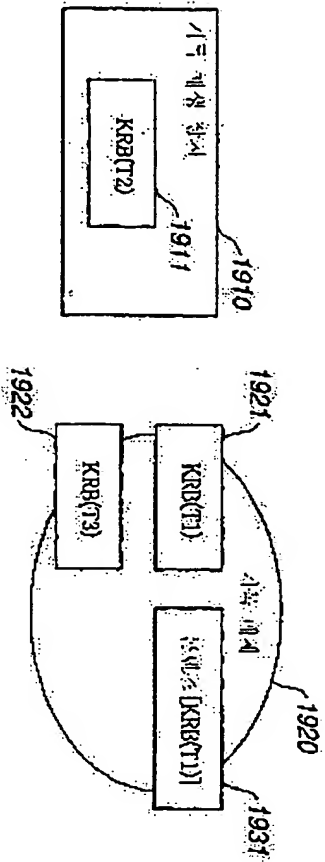
도면 17



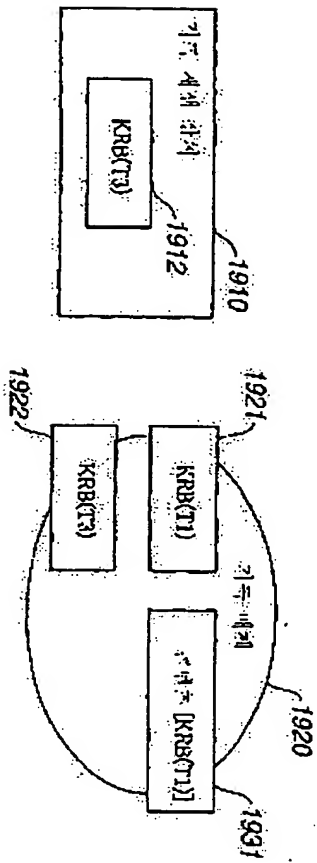
도면 18



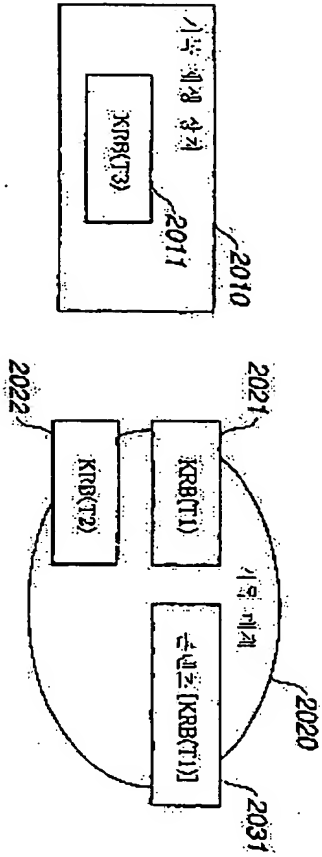
도면 191

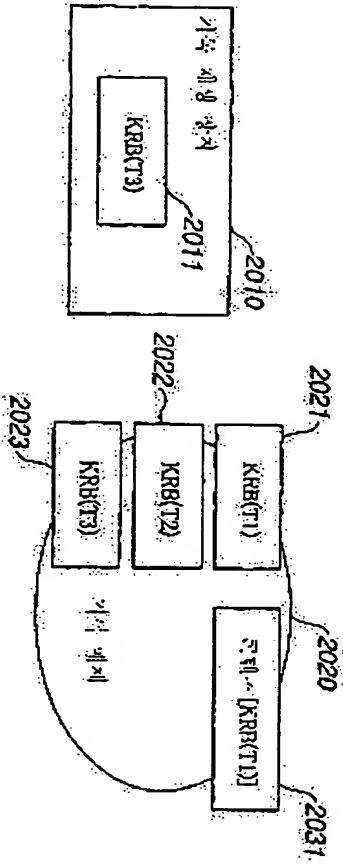


도면 185

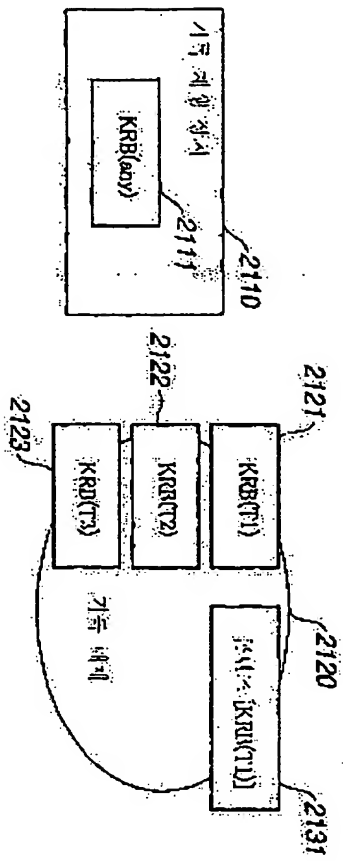


도 201

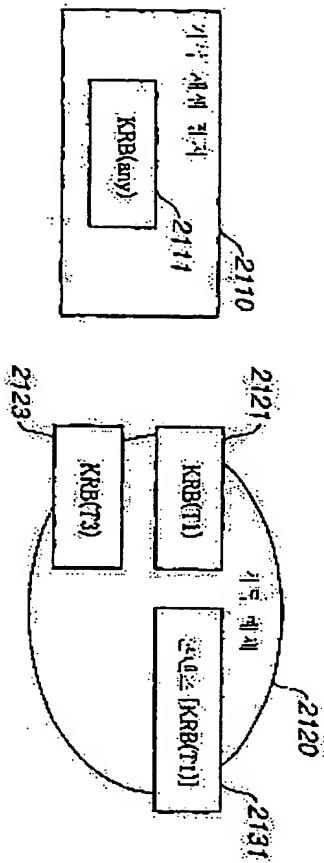




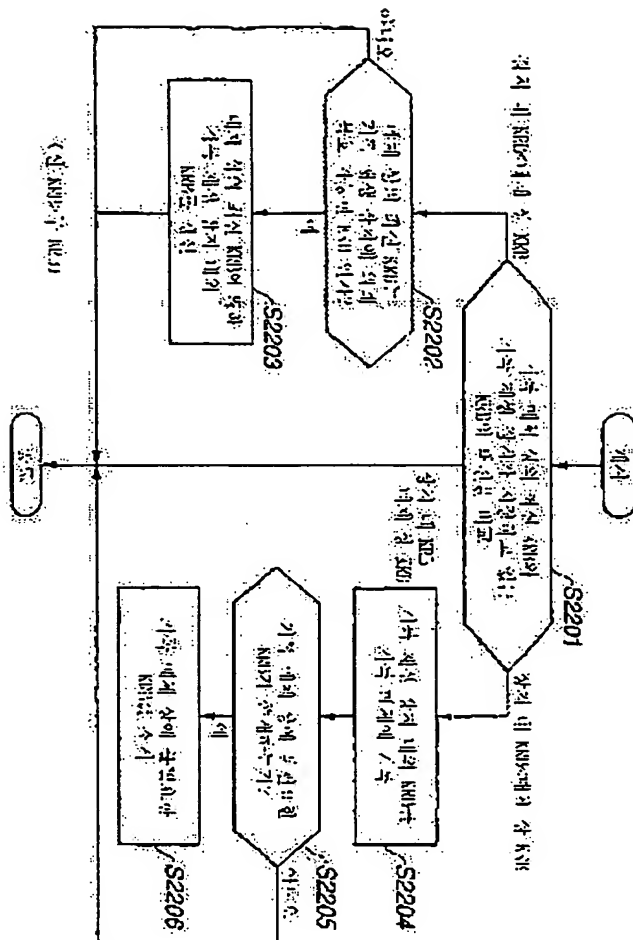
도면21A



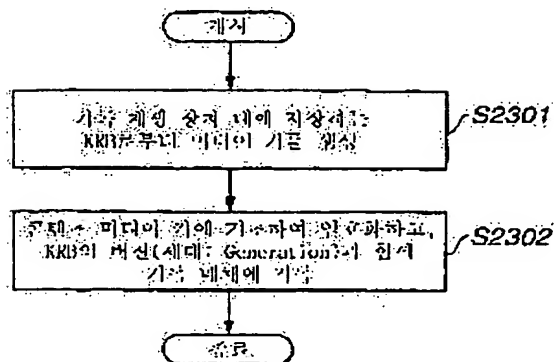
도면218



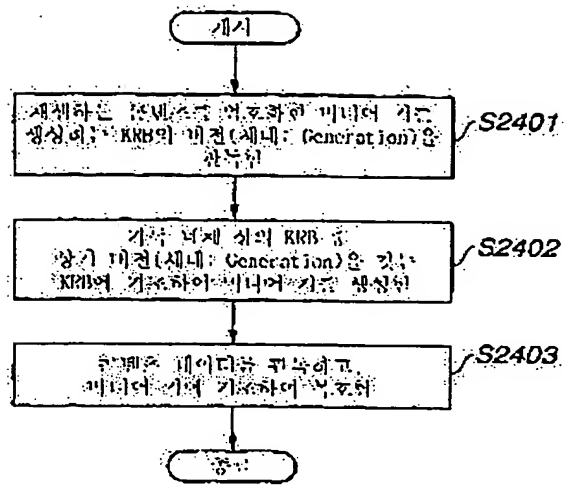
도면22



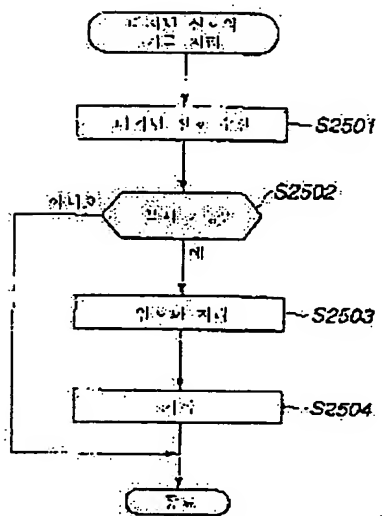
DP23



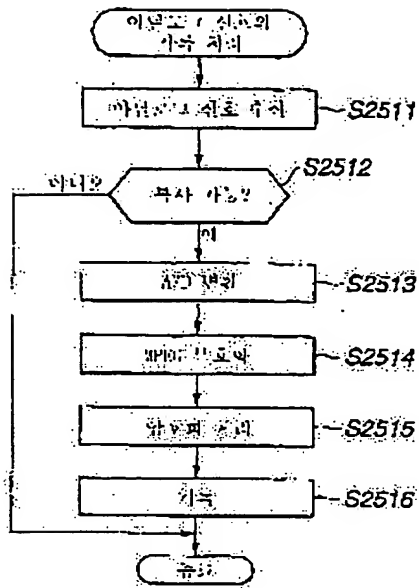
도면24



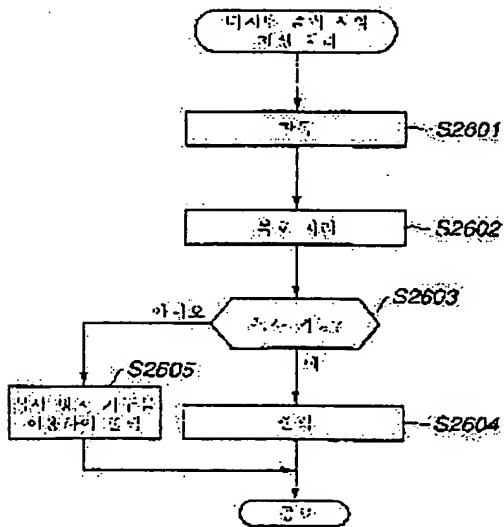
도면25A



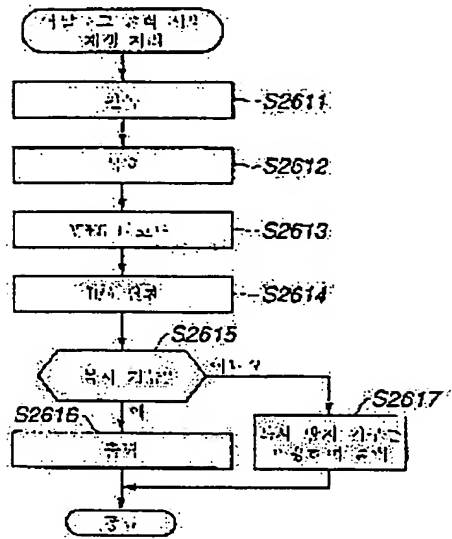
도면258



도면259



도면 238



도 27

